Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

Distributed Estimation based Public Key Infrastructure for In-vehicle network security

Karthika Venkatesan 1, Seshadhri Srinivasan 2, Padmapritha Thamotharan 3, Nimesh Nagar 1, Haribabu P 1, S D Sudarsan 1, K K Soundara Pandian 4.

1. C-DAC, Bangalore
2. TVS Sensing Solutions PVT Ltd
3. Kalasalingam Academy of Research and Education
4. CCA, Government of India

C-DAC

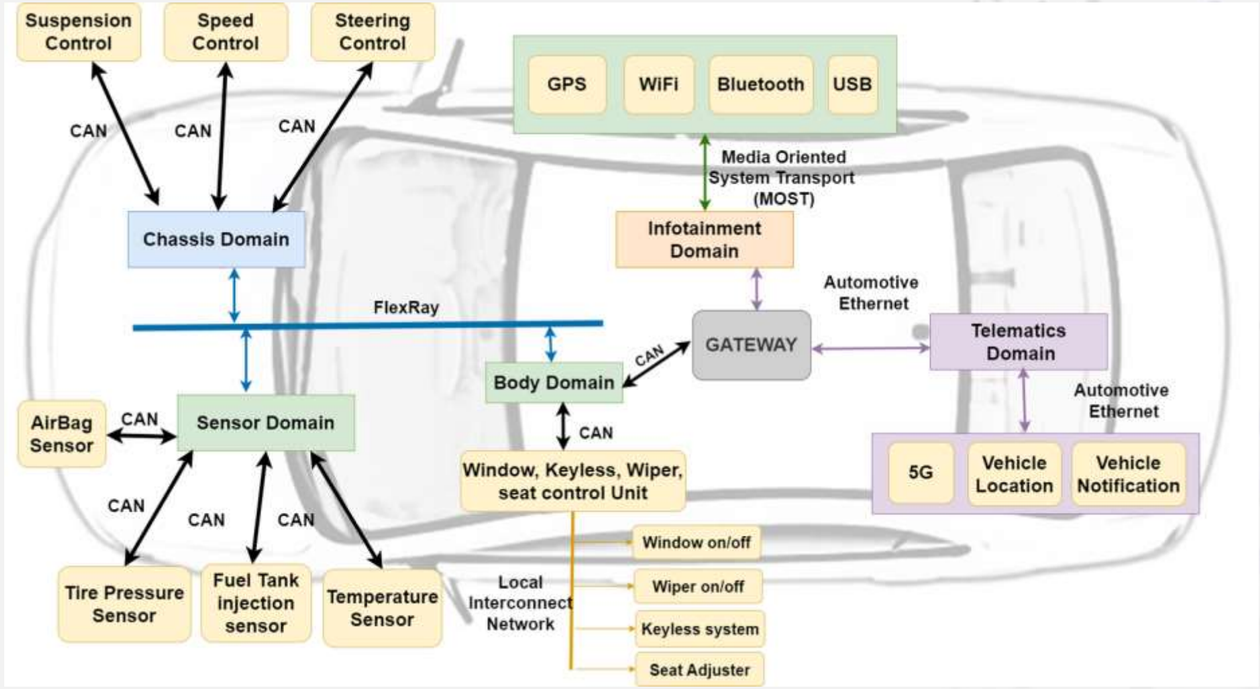
https://pkiindia.in

Social Media /pkiindia

IEEE BANGALORE SECTION

CURRENT SCENARIO

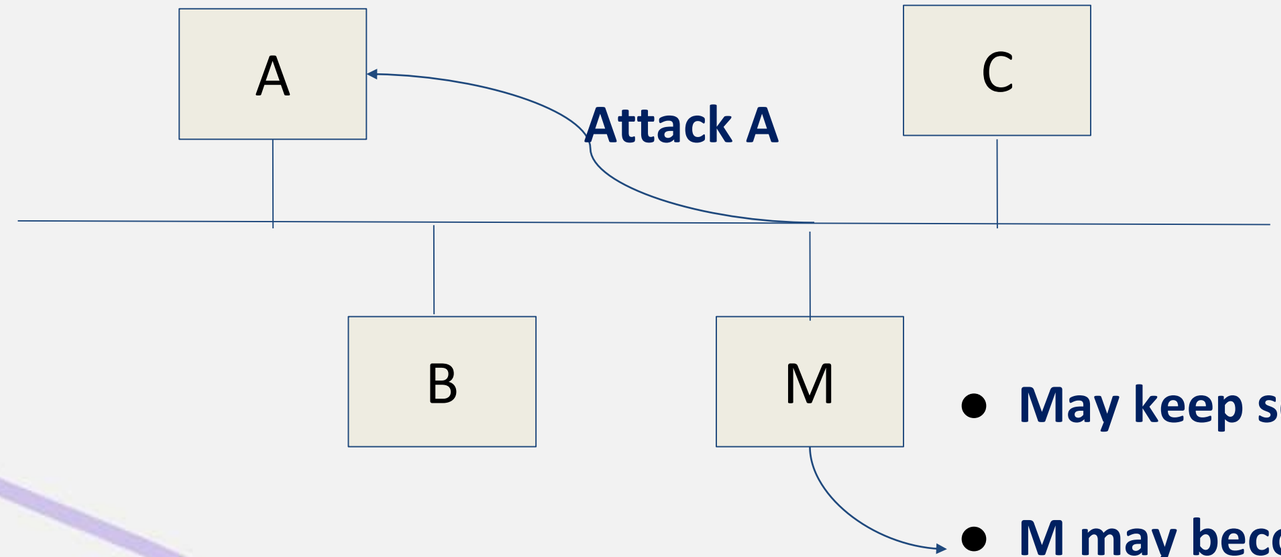
- In-vehicle network comprises of at least 70+ ECUs with other components
- Lightweight cryptographic schemes are well appreciated and are being researched
- Identity of these components becomes important



Cyber physical systems - have large number of Cyber Physical variables - that are dynamic, continuously changing

PROBLEM STATEMENT

- ECUs are responsible for controlling the functionalities of Car- engine controls, transmission, brakes etc.



- May keep sending data to A,
- M may become malicious by firmware update or newly introduced node

CURRENT SCENARIO

How can A ensure M is genuine node?

- **M can be a device spoof**
- **M can try to create more garbage data**

A has to decide if it can trust M.

Cryptographic mechanisms, key changes are possible but comes with the concern of working on microcontrollers with limited hardware and should also fast enough

Can we leverage the existing cyber physical data of these components over the network & propose a mechanism to ensure layer of security?

→ **DISTRIBUTED ESTIMATION BASED PKI**

Contd..

Let us consider a network

E1
E2
E3

Each of these ECUs contains CPS variables

- E1- Temperature
- E2 - Speed
- E3 - Odometer values

- It may even contain combination of CPS variables
- If a device M contains info and E3 wants to verify, How can it do before consuming the data

Concept of Relative Measurements

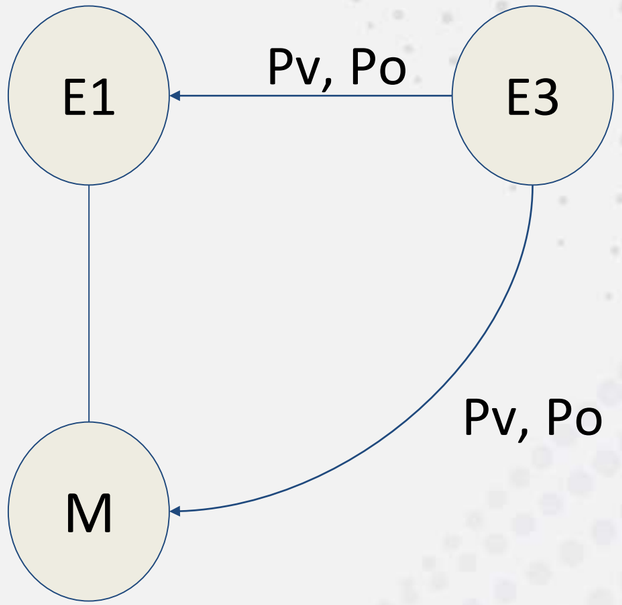
- A node will always know the relative measurement with its nearest neighbours
- Consider that there are 3 nodes - N1, N2 and N3
  - N1 is the neighbour of N2
  - N2 is a neighbour to N3
- All 3 of them holds temperature values
  - Range of N1 is 0-40 degrees
  - Range of N2 is 0-80 degrees
  - Range of N3 is 20-30 degrees

Concept of Relative Measurements

- N1 knows N2 can either have value equivalent to N2 or can have values which may vary utmost by 40 degrees . N1=N2 or N2-N1 <= 80
- N1 knows N2 can either have value equivalent to N2 or can have values which may vary utmost by 40 degrees . N1=N2 or N2-N1 <= 80
- Here relative measurement of N3 wrt to N2 is N2=N3 or N3-N2>19 and N3-N2<61
- Similarly N2 relative measurement with respect to N1 and N3.
- These relative expressions are dynamic, so that data can be asked for a specific time point. At any given point N1 will contain value +2 [that means its value is N2+2]
- If N3 is trying to connect to N1, N1 can know the relative measurement of N3 via N2 as well as, ask N3 to provide its relative measurement to N2

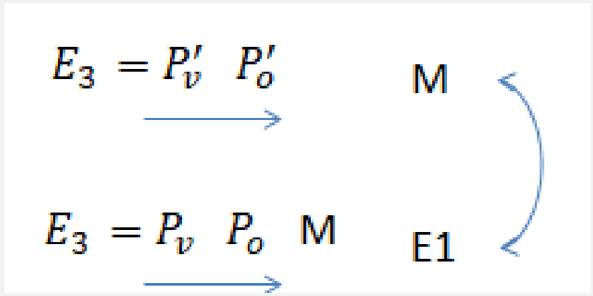
GRAPH BASED ESTIMATION TECHNIQUE

- We use a graph structure for the ECU network & it can be based on trust/network topology - stored in the trusted root (TR)
- We create a probing vector and probing sequence
- Probing Vector(Pv):
  - Vector of cyber physical variables : {Speed, temperature, timestamp}
- Probing Order(Po) - a sequence to be used for probing among these variables
- E3 sends Pv, Po to the TR along with M, to check for the path through which probing can happen
- TR returns back the 1 hop neighbour of M - the node E1.



CASE 1 - Node E1 is trusted node by E3

- E3 asks for the relative measurement of Pv, Po to E1 with respect to node M
- E3 asks for relative measurement of Pv', Po' to node M, with respect to E1
- If the relative measurements match, then the node is safe to communicate
- Else, the node M, may be suggested for isolation to trusted root



Results are compared

If it's OK, E3 trusts M

$P_v' \quad P_o'$ A modified probe vector & Order

CASE 2 - Node E1 is not-trusted node by E3

- E3 keeps recursively probing via TR to receive its trusted node, this forms a subgraphs of paths to E1 via trusted nodes {T1, T2, T3}
- E3 can pick any trusted node to ask for relative measurement again until it gets the relative measurement of M with respect to either T1 or T2 or T3.
- It can even ask such measurement to two of its trusted nodes, to be sure.

CASE 3 - Trusted Root does not know about M

- TR will inform M is not trusted device
- Further actions can be taken based on PKI mechanisms

DISTRIBUTED ESTIMATION BASED PKI

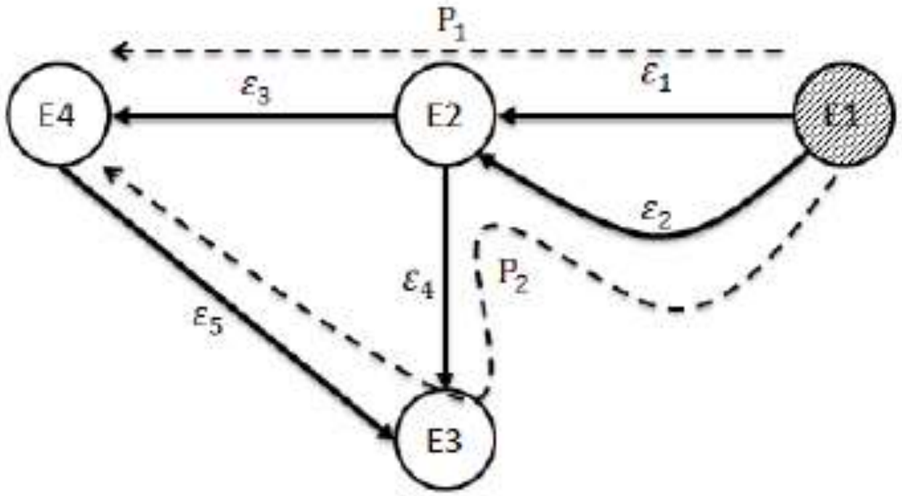
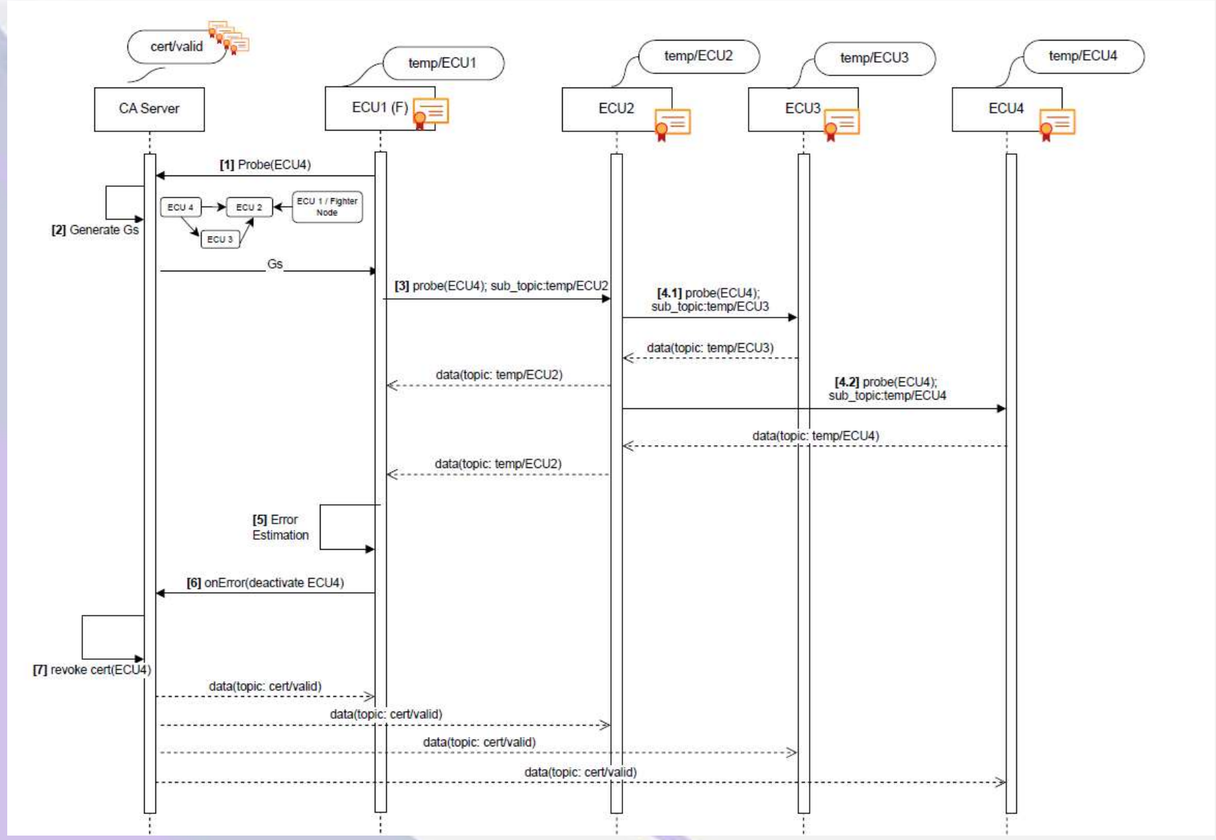


Fig. 4. ECU Network Model

- A vector of CPS variables is used for probing vector with probing order.
- So they will not be linear measurements or relationships for others to easily identify the same

IMPLEMENTATION



The ECU1, ECU2, ECU3 and ECU4 publish the temperature data through their respective topics temp/ECU1, temp/ECU2, temp/ECU3 and temp/ECU4 respectively.

THANK YOU