ICIMP 2023 Presentation

Performance Evaluation of an Authentication Scheme for IoT Networks

Presented by: Chi Ho Lau (Tommy)

City University of Hong Kong, China
chihlau-c@my.cityu.edu.hk

香港城市大學
City University of Hong Kong

Outline

- IoT networks consist of many devices that collect information about us
  - Authentication issue
- Overview of the Blockchain-based authentication scheme
- Performance evaluation
- Numerical Results
- Conclusion

Background
IoT networks

- IoT devices are **heterogeneous** in nature
- Connected to the **Internet**
- IoT networks are **huge** in size
- Embedded with **sensors**, **software**, and **other technologies**
- A building block of **automation**
  - Smart manufacturing
  - Smart power grids
  - Smart cities – the self-driving car
  - Medical

Problems

Source: http://www.insecam.org/

- Internet of Things (IoT) networks are huge in size
- IoT networks have access to sensitive data
- “A very popular vector for gaining access to IoT devices arises due to inadequate authentication and authorization procedures.” [1]
- Difficult to assess the performance of an authentication scheme
- Formal analysis does not provide quantitative results for comparison

[1] Mohamad Noor, M. B., & Hassan, W. H. (2019). Current research on internet of things (IoT) security: A survey. Computer Networks, 148, 283-294.

Background
Blockchain

- Blockchain is a **decentralized storage solution**
- Blocks are linked in **chronological order** by their digital fingerprint
- Difficult to **forge blocks or records**
- Coin-based blockchain system
  - **Bitcoin**, **Ethereum**, etc...
- The evaluated authentication scheme is based on **coins**
- Every device has a unique **device identifier (Id)**

Background
Block structure

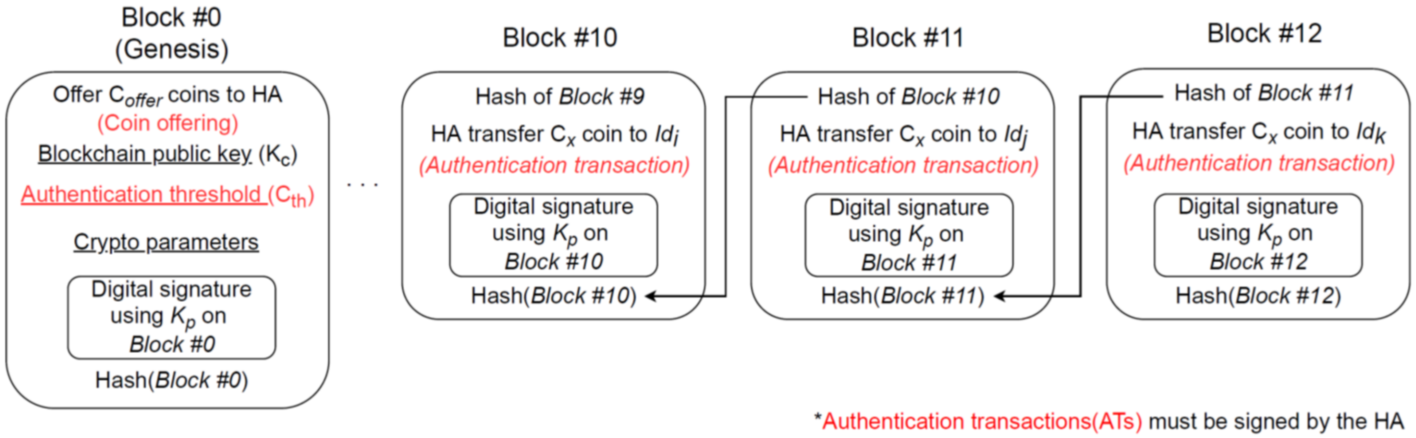
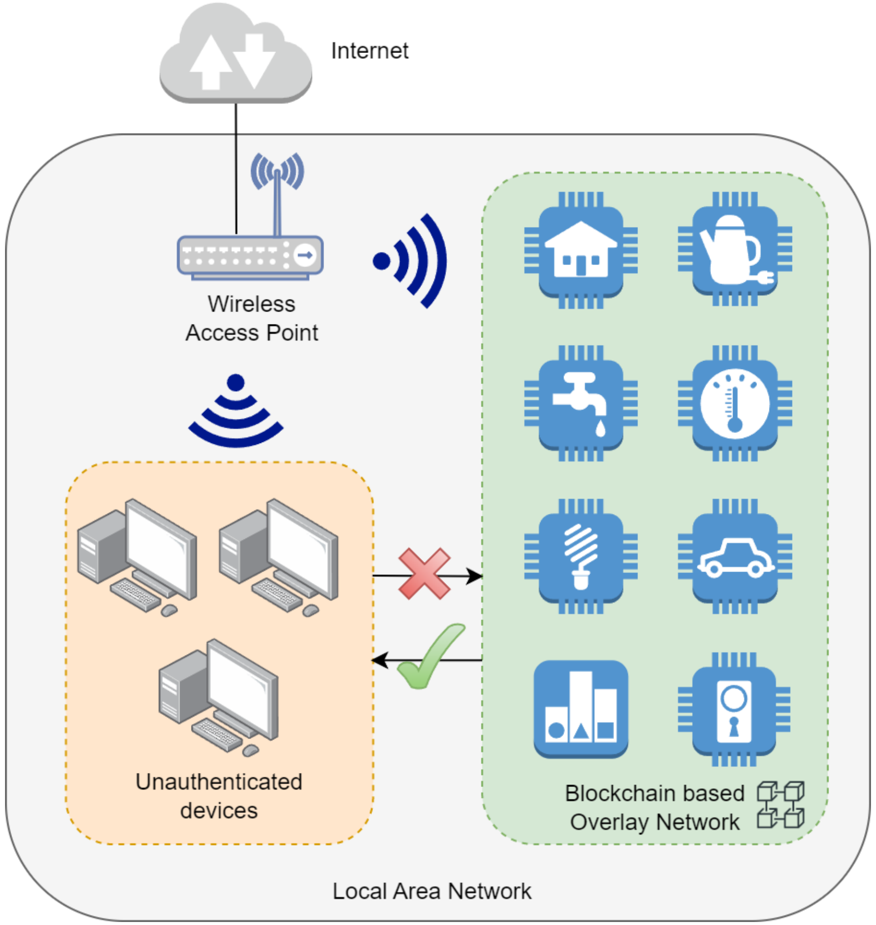


Fig. 2. Structure of Authentication Blockchain

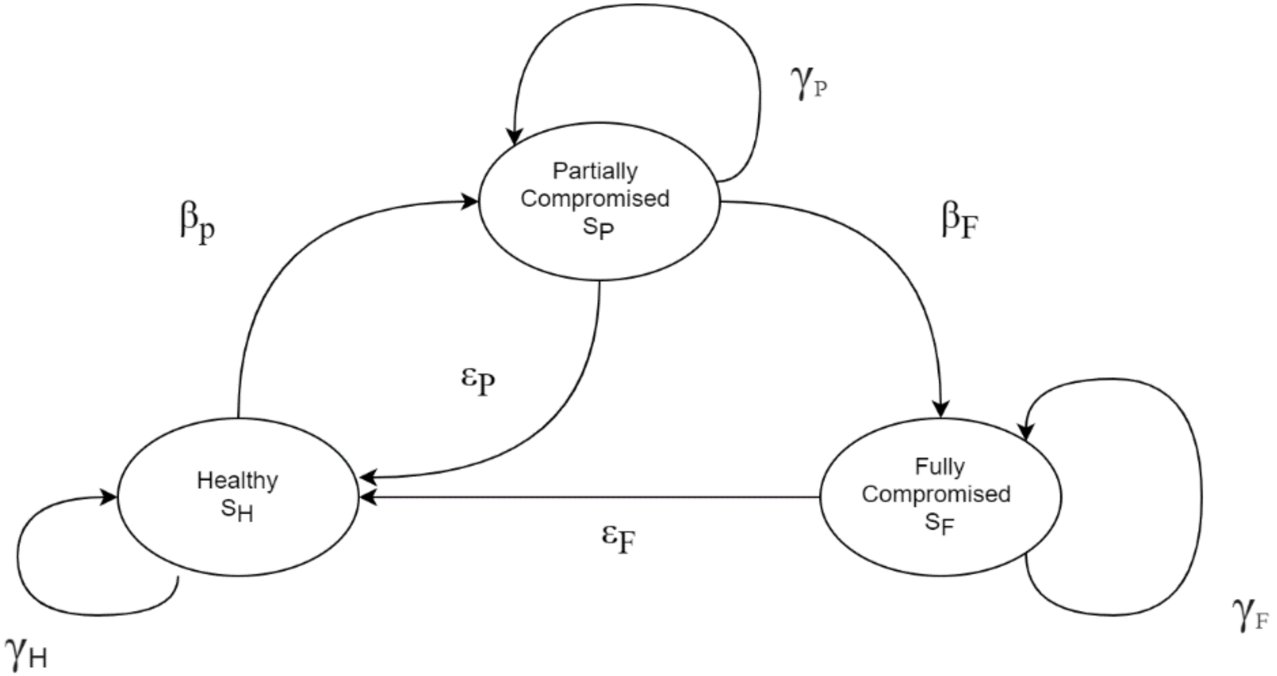
- Genesis block contains **Blockchain public key (*k_c*)**
- Configure the **authentication threshold (AT)**
- Each block has the **digital signature** of **HA**
- Digital signatures were produced by **Blockchain private key (*k_p*)**

Blockchain-based Authentication scheme



- Every IoT device has a unique **device identifier (Id)**
- Hardware authenticator (HA) has initial coins
    - Kept by the **network administrator**
    - No **internet access**
- Authenticated IoTs receive a certain number of **coins** from HA
- Own certain number of coins are **considered authenticated**
- Authenticated IoTs talk to each other only
- Forming an **overlay network**

Stochastic Threat model



Markov Diagram

Transition probability matrix :

$$P = \begin{Vmatrix} \gamma_H & \beta_p & 0 \\ \varepsilon_P & \gamma_P & \beta_F \\ \varepsilon_F & 0 & \gamma_F \end{Vmatrix}$$

β = Move to the next state
γ = Stay at the current state
ε = Recover to previous state

Stochastic Threat model – cont.

- Put a Markov process $\{X_n\}$ in the long run such that $n \rightarrow \infty$, the probability for each state *j* will converge to a limiting probability (π_j)

$$\pi_j = \lim_{n\to\infty} \Pr\{X_n = j | X_0 = i\} \qquad for\ i, j = 0, 1, 2.$$

- By substituting the transition probability matrix (P):

$$\pi_0 = \frac{\varepsilon_F(1-\gamma_P)}{\varepsilon_F(1-\gamma_P) + \beta_p(\varepsilon_F + \beta_F)}$$

$$\pi_1 = \frac{\beta_P\varepsilon_F}{\varepsilon_F(1-\gamma_P) + \beta_p(\varepsilon_F + \beta_F)}$$

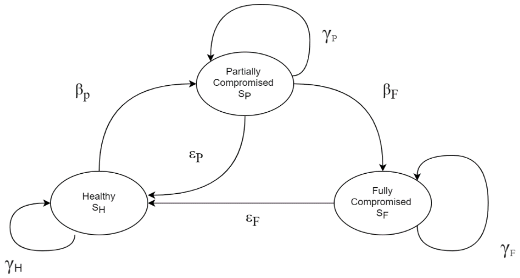
$$\pi_2 = \frac{\beta_P\beta_F}{\varepsilon_F(1-\gamma_P) + \beta_p(\varepsilon_F + \beta_F)}$$

$$P = \begin{Vmatrix} \gamma_H & \beta_p & 0 \\ \varepsilon_P & \gamma_P & \beta_F \\ \varepsilon_F & 0 & \gamma_F \end{Vmatrix}$$

- π_j consists of four parameters: β_P, β_F, γ_P, ε_F

Solving the model

- Classify the vulnerabilities between 2008-2016 into 2 levels that causing
  - Partially compromised state (V_P)
  - Fully compromised (V_F)
- Assume the average exploitation rate for V_p be E_p and V_F be E_F.
- Therefore, $\beta_P = E_p V_P$ and $\beta_F = E_F V_F$.



Type of vulnerability	Count	Percentage	Level	Possible attack
Format String Vulnerability	110	0.294709	V_F	- Execute arbitrary code
Configuration	195	0.522438	V_P/V_F	- Exposure of config file - Execute arbitrary code
OS Command Injections	208	0.557267	V_F	- Execute arbitrary code
Race Conditions	377	1.010047	V_F	- Privilege escalation
Link Following	389	1.042197	V_F	- Privilege escalation
Credentials Management	589	1.578031	V_F	- Privilege escalation
Cryptographic Issues	779	2.087073	V_P / V_F	- Information leakage - Password leakage
Authentication Issues	920	2.464836	V_P / V_F	- Information leakage - Privilege escalation
Cross-Site Request Forgery (CSRF)	1161	3.110516	V_P	- Information leakage
Numeric Errors	1199	3.212324	V_F	- Privilege escalation
Code Injection	1545	4.139317	V_F	- Execute arbitrary code
Path Traversal	1686	4.51708	V_P	- Information leakage
Information Leak / Disclosure	2939	7.874079	V_P	- Information leakage
Input Validation	3763	10.08171	V_P / V_F	- Information leakage - Execute arbitrary code
SQL Injection	3828	10.25586	V_P / V_F	- Information leakage - Execute arbitrary code
Permissions, Privileges, and Access	4661	12.48761	V_F	- Privilege escalation
Cross-Site Scripting (XSS)	6220	16.66443	V_P	- Information leakage
Buffer Errors	6756	18.10047	V_F	- Privilege escalation
Total	37325	100	V_P =57.57 V_F =67.83	

Table. 1: Vulnerability counts and categories from 2008-2016

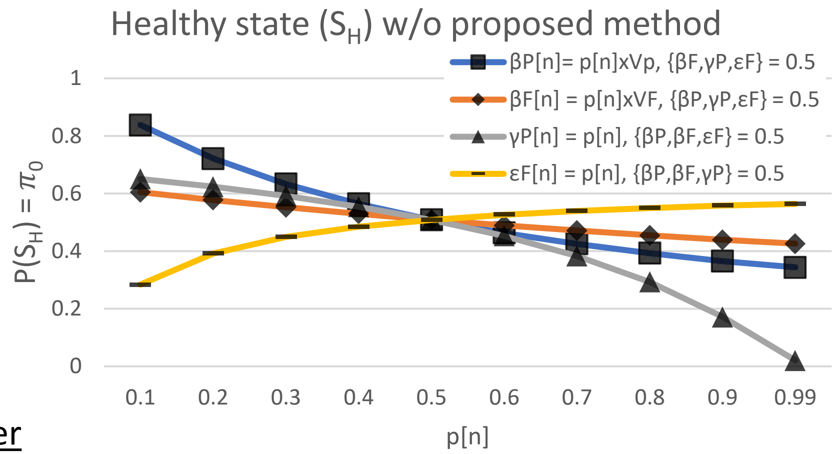
香港城市大學 City University of Hong Kong

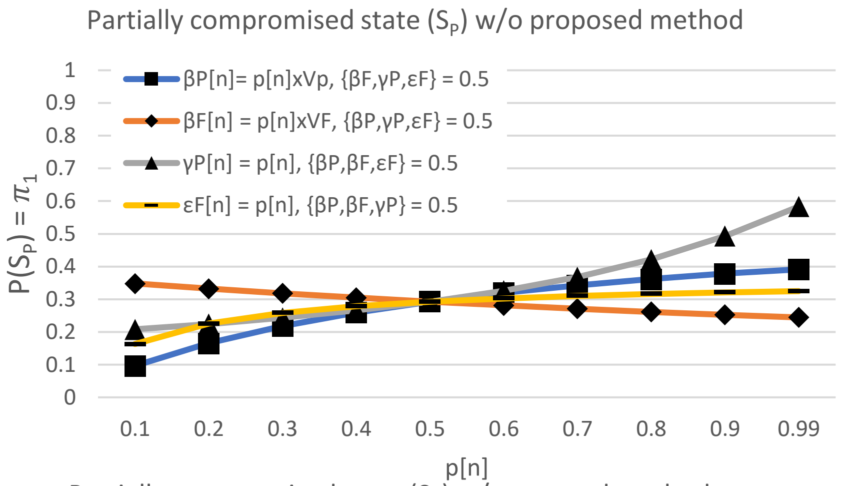
Numerical Results – Cont.

β = Move to the next state
γ = Stay at the current state
ε = Recover to previous state

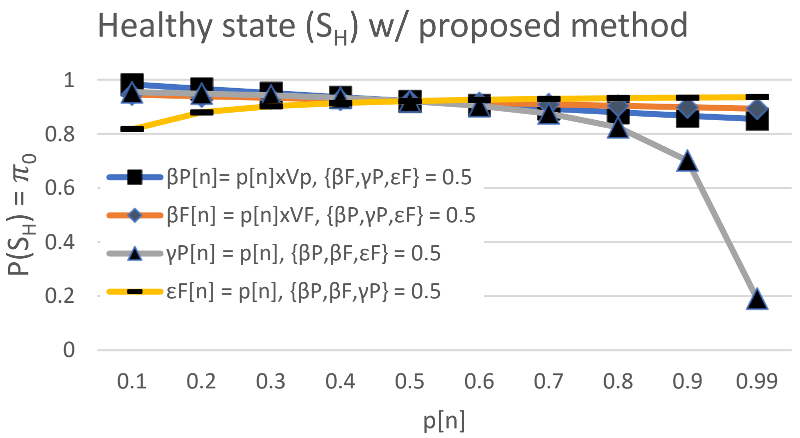
$$p[n] = \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.99\}$$

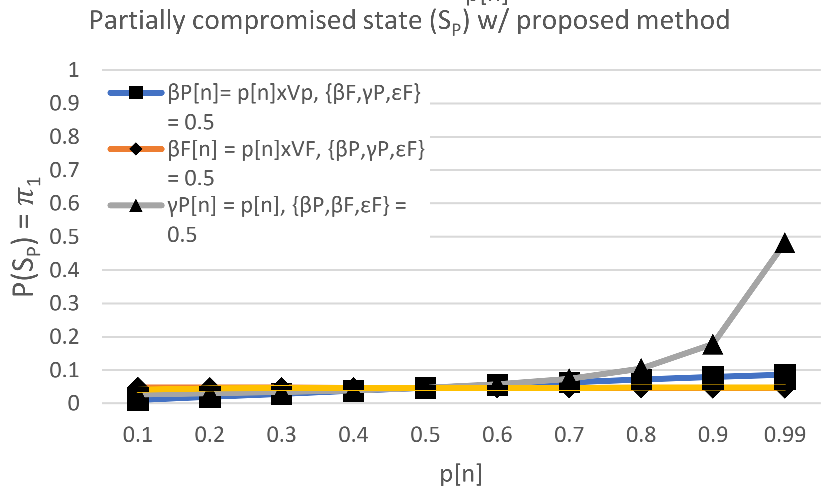
Higher is better





Lower is better

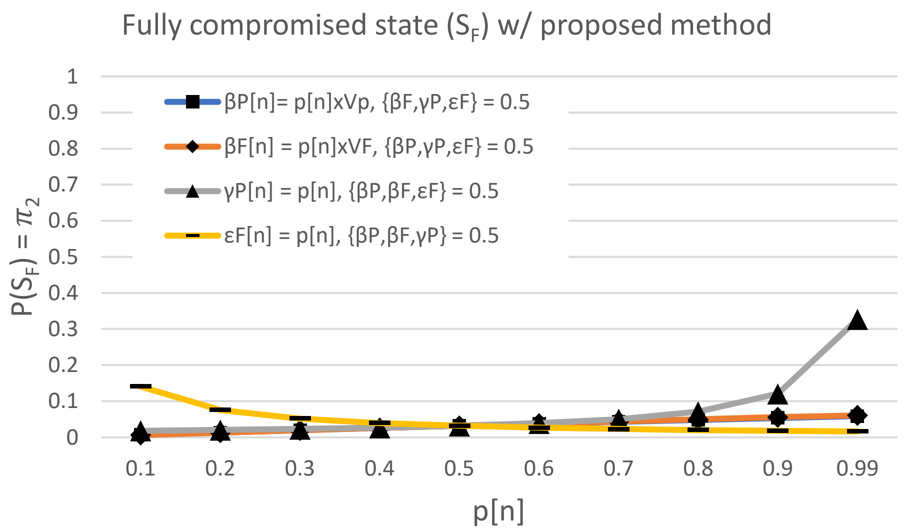




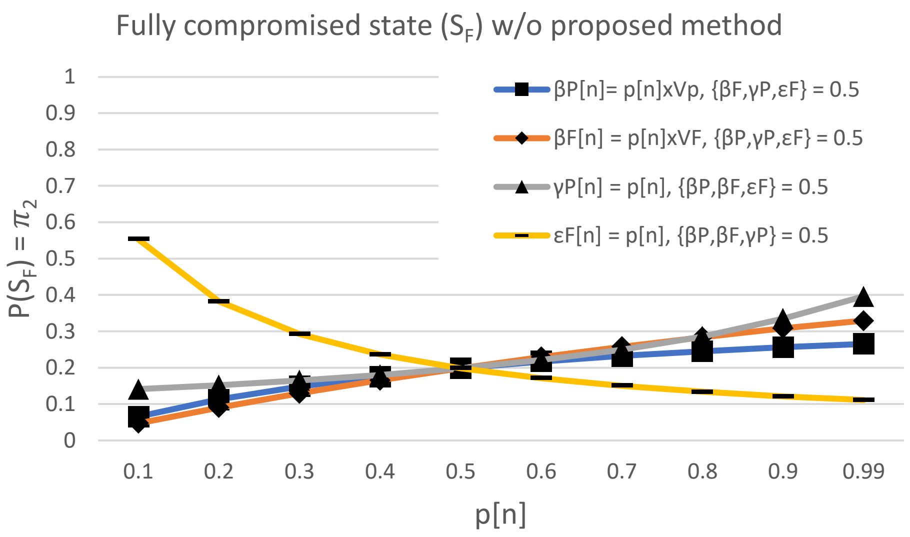
香港城市大學
City University of Hong Kong

Numerical Results – Cont.

β = Move to the next state
γ = Stay at the current state
ε = Recover to previous state



Lower is better



Lower is better

$$p[n] = \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.99\}$$

Summary

	Without proposed method	With proposed method	Difference
Average π_0 (Healthy state)	0.4852	0.8911	+83.66%
Average π_1 (Partially compromised state)	0.2989	0.0625	-79.09%
Average π_2 (Fully compromised state)	0.2158	0.0463	-78.53%

Average improvement	80.43%

- Blockchain-based authentication scheme can greatly improve the IoT security level