Zero Trust Architecutre for 6G Security

Chuen, X., Feng, W., Ge, N., Zhang, Y.

IEEE Network 2023

2024.03.14.

Summarized by, Sangwi Kang | swkang@mmlab.snu.ac.kr

Outline

- Introduction
- Challenges in 6G Security
- Zero Trust Architecture
- Zero Trust Architecture for 6G Networks
- Limitations of ZTA on 6G
- ZTA-6G : A Software-Defined ZTA for 6G Security
- Evaluation
- Conclusion

Introduction

- The primary goal of 6G network is to establish seamless global connectivity for billions of entities
- There are **many security vulnerablilities** on 6G network
  - Billions of entities, open-source softwares, diverse attack surfaces, etc.
- Conventional security solutions are **inadequate for 6G**

- In this paper, a collaborative **Zero Trust Architecture (ZTA)** for 6G networks is proposed to address these issues

Challenges in 6G Security

- The various factors pose security threats in 6G networks
  - Network openness, virtualization, containerization, adversarial machine learning, etc.

- **Ultra large scale** : Traditional high-complexity architectures may not be effective for 6G scale
- **Heterogeneity(HetNets)** : Multiple operators, control domains introduce complexities
- **Openness** : O-RAN(Open Radio Access Network) causes more complexity and integration difficulty
- **Autonomous Interactivity** : The autonomous M2M(Machine-to-Machine) interactions should be monitor more carefully

Zero Trust Architecture

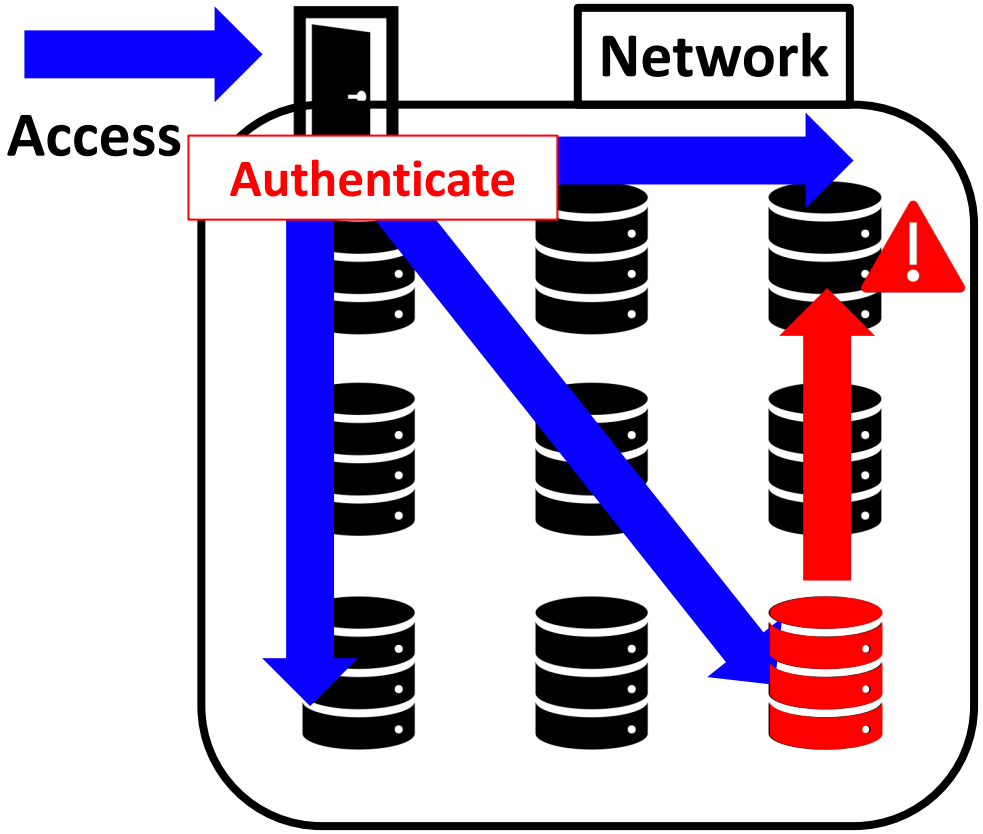

Authenticated

Zero Trust Architecture (ZTA)

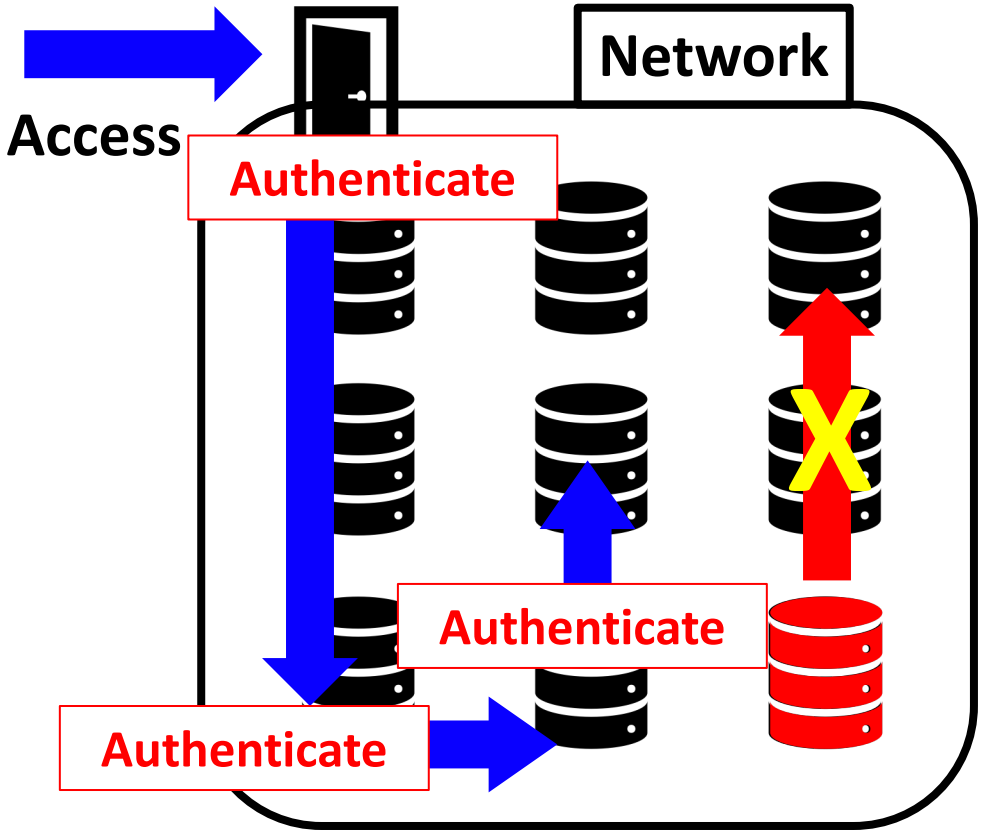
> Concept

- In one sentence, ZTA is ***"Never trust and always verify"***

Network-based Access Control



Zero Trust Network Architecture



Zero Trust Architecture (ZTA)

> History (from Wikipedia)

- In April 1994, the term "zero trust" was coined by Stephen Paul Marsh in his doctoral thesis on computer security at the University of Stirling

- In 2010 the term zero trust model was used by analyst John Kindervag of Forrester Research to denote stricter cybersecurity programs and access control **within corporations**

- In 2018, work undertaken in the United States by cybersecurity researchers at NIST and NCCoE led to the publication of **NIST SP 800-207 – Zero Trust Architecture**

Zero Trust Architecture (ZTA)

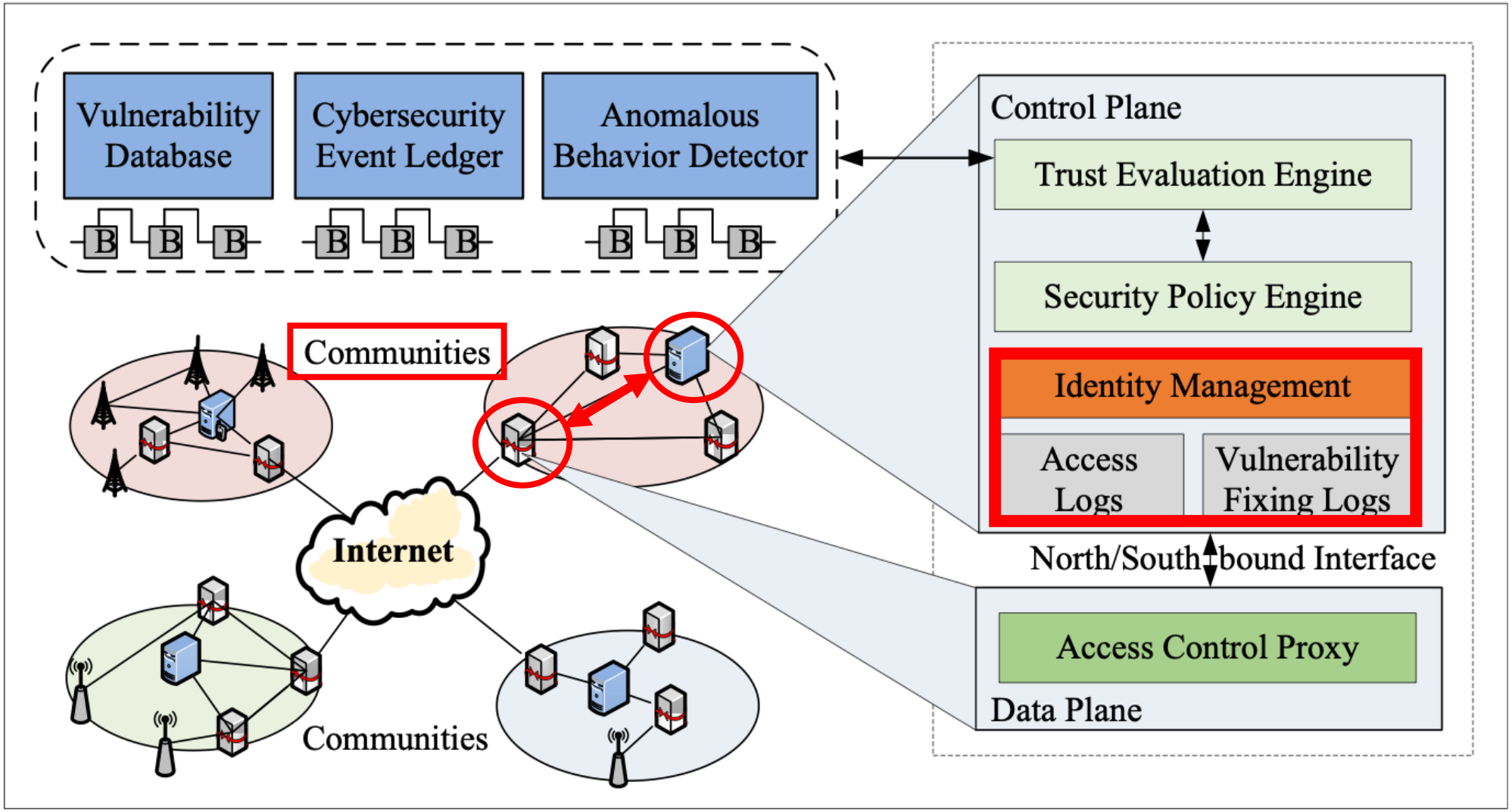
> Trends of ZTA

- In 2019, the U.K. National Cyber Security Centre recommended that network architects **consider a zero trust approach** for new IT deployments, particularly where significant use of cloud services is planned.
- U.S. President Joe Biden issued Executive Order on **Improving the Nation's Cybersecurity** 10428 in May 2021

- The South Korean government recommends the following strategies for applying the zero trust model
  - 국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립 - 대한민국 대통령실, 2024.2.
  - 과기정통부, 제로트러스트 가이드라인1.0 발표 - 과학기술정보통신부, 2023.7.
  - 2026년부터 정부 숑기관에 K-제로 트러스트 적용된다 - 언론사 초청 사이버안보 간담회, 국가정보원, 2023.7.

Zero Trust Networks, NIST Zero trust security model, Wikipedia 제로트러스트 가이드라인 1.0, KISA
제로 트러스트(Zero Trust), 보안과 신뢰의 고정관념을 깨다, SAMSUNG SDS

Zero Trust Architecture for 6G Networks



Limitations of ZTA on 6G

- Fine-grained access control strategies

  ⟷ The scale and complexity of 6G networks

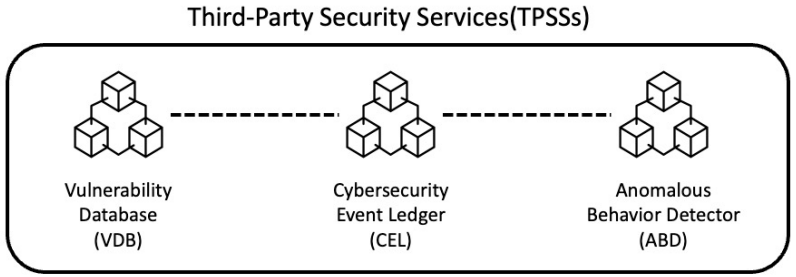
- Centralized controller for single network domains

  ⟷ The decentralized management architectures of 6G networks

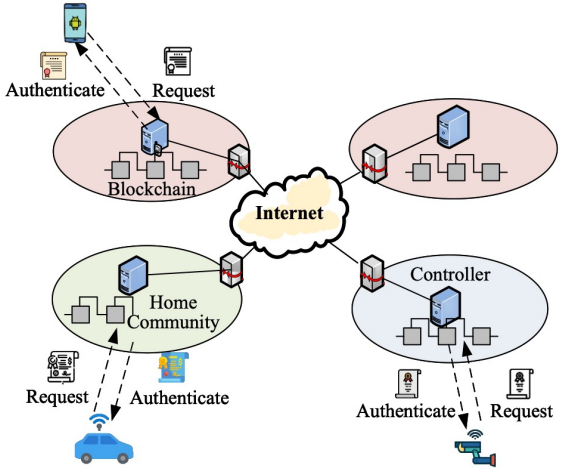
- End-to-end encryption

  ⟷ Resource constrained IoT in 6G

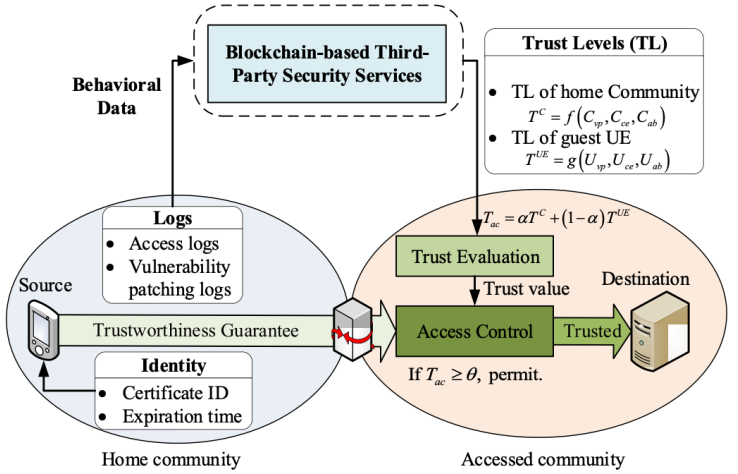
ZTA-6G : A Software-Defined ZTA for 6G Security



Distributed Security Architecture



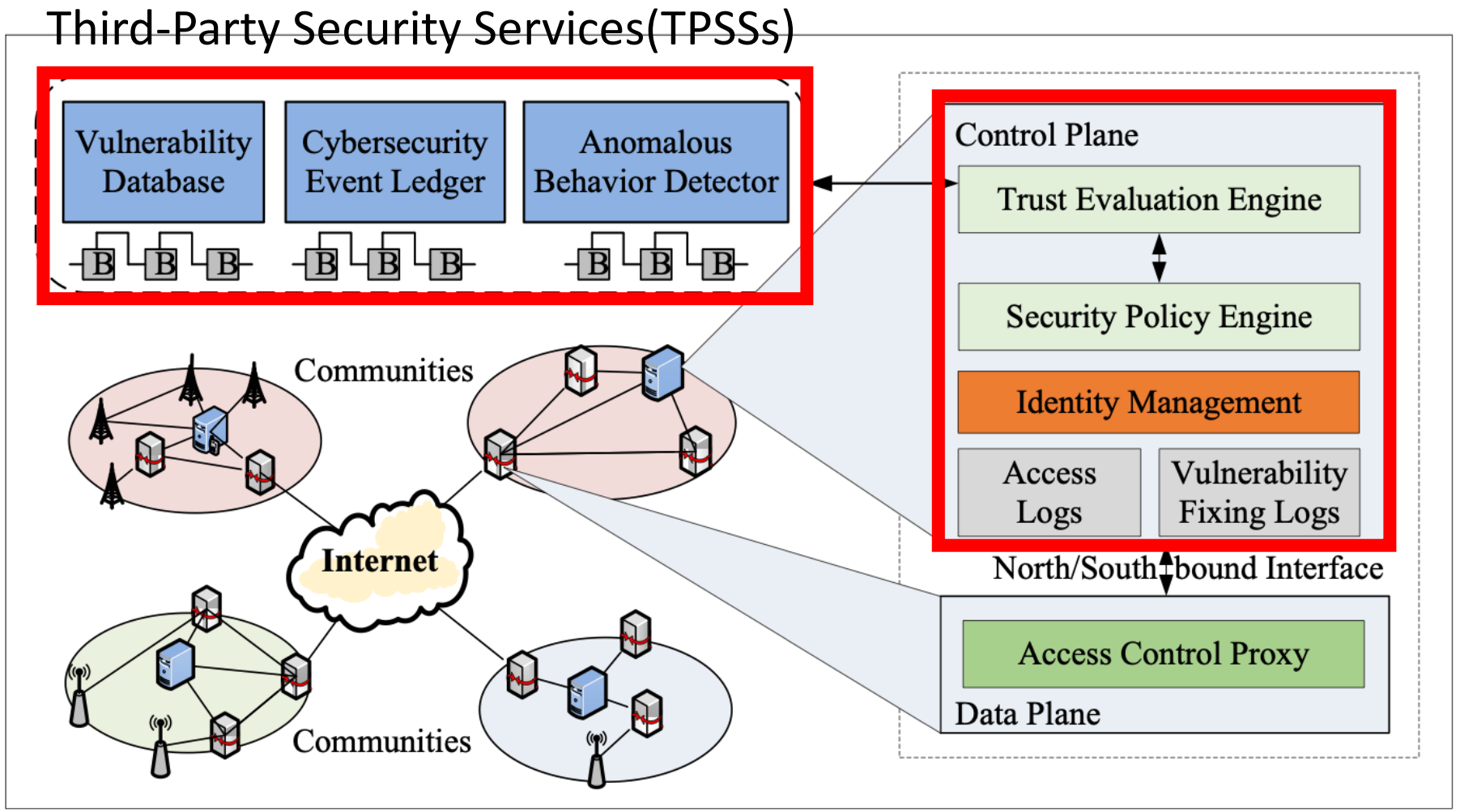
Decentralized Identity Management



Trust Evaluation System

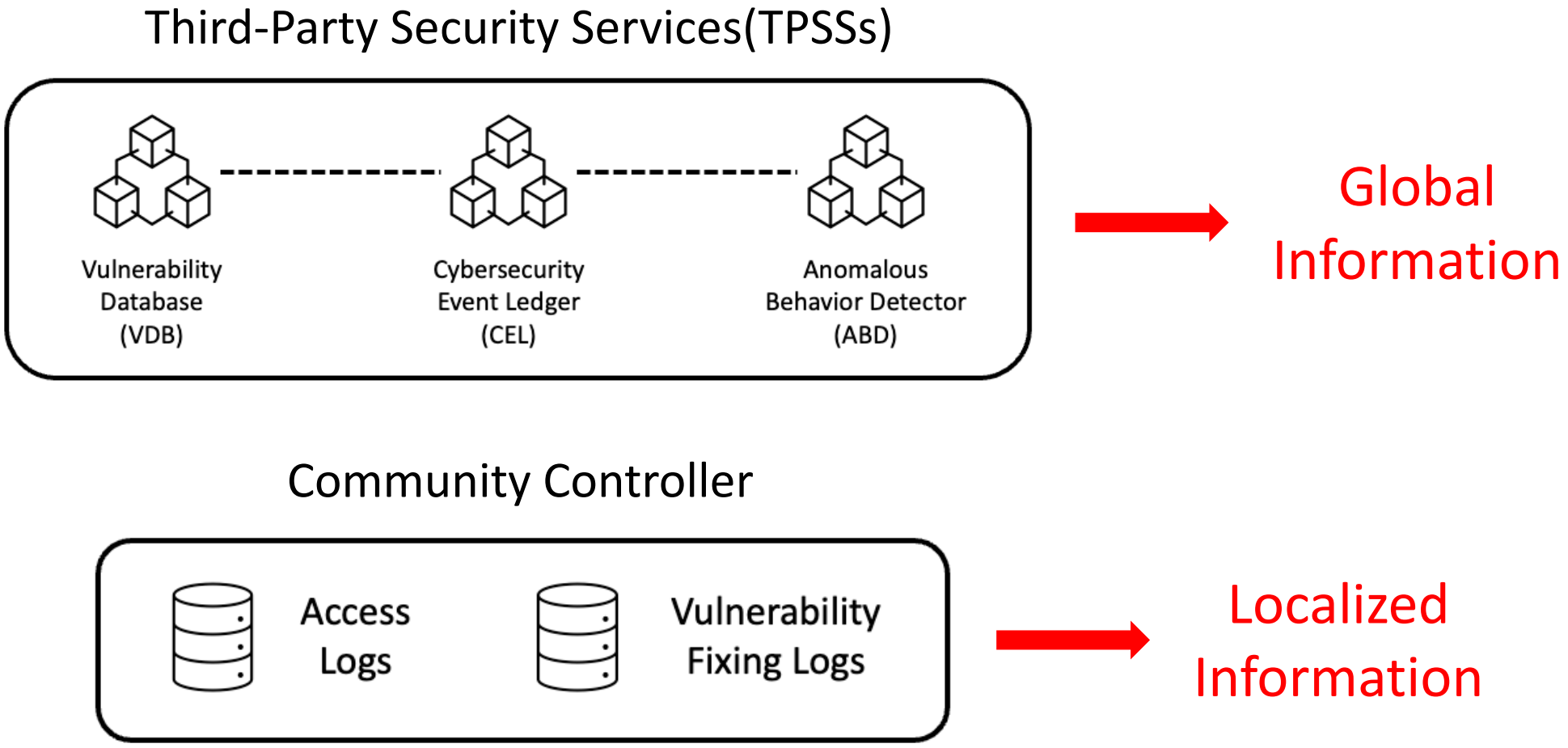
ZTA-6G : A Software-Defined ZTA for 6G Security

> Distributed Security Architecture (1)



ZTA-6G : A Software-Defined ZTA for 6G Security

> Distributed Security Architecture (2)



ZTA-6G : A Software-Defined ZTA for 6G Security

> Decentralized Identity Management (1)

- In 6G, it is very difficult to establish and maintain **a unified identity system** due to more diversified network environments
- Traditional identity authentication schemes based on data certificates cannot satisfy the requirements of access control in 6G

- Unified CA(Certification Authority) → Scalability limits
- Multiple CA → Mutual trust problem
- Totally distributed ID management → Too many certificates

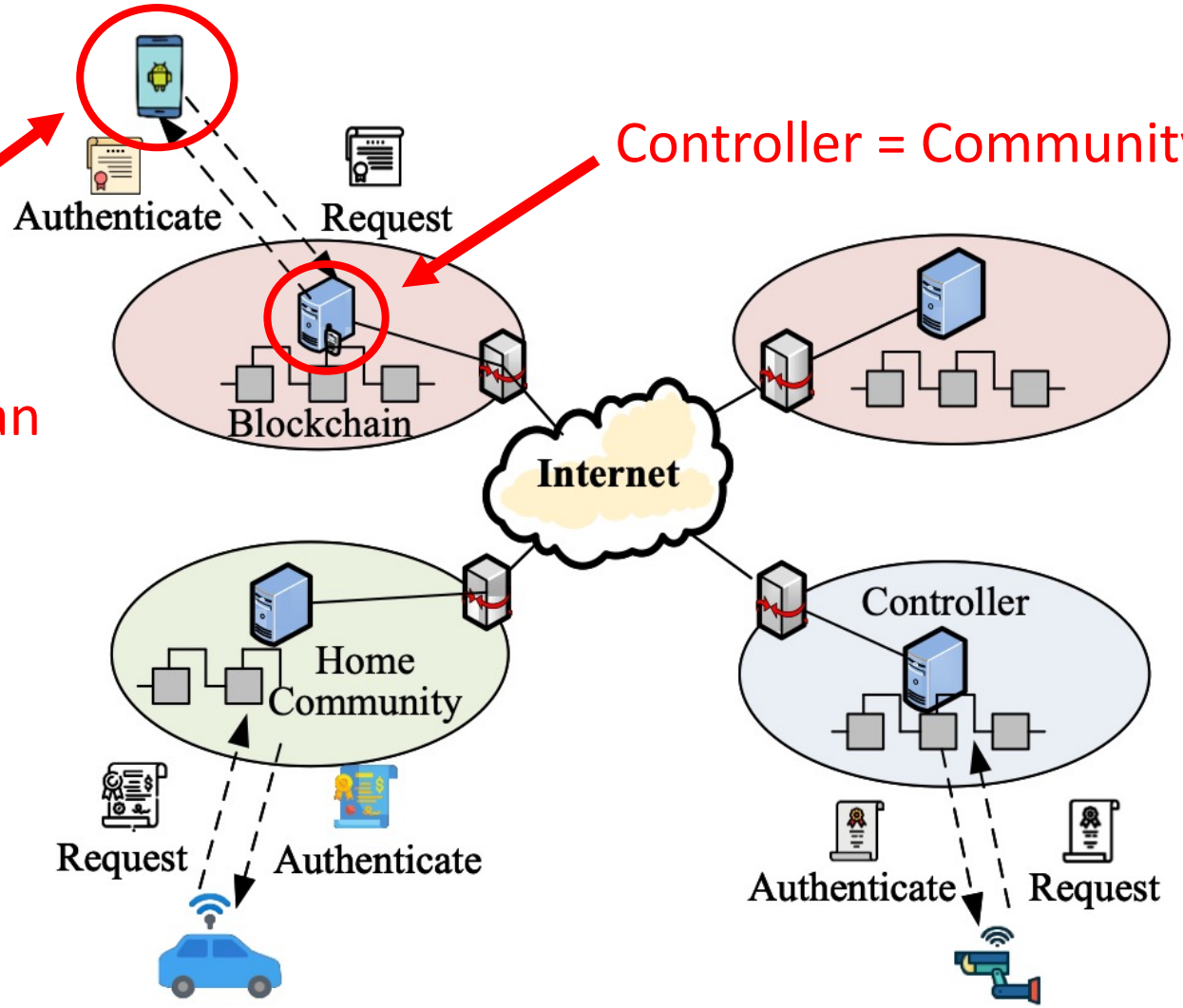
- Proposed solution : **Decentralized Identity Management**

ZTA-6G : A Software-Defined ZTA for 6G Security

> Decentralized Identity Management (2)

UE(and Controller) can generate the cert.

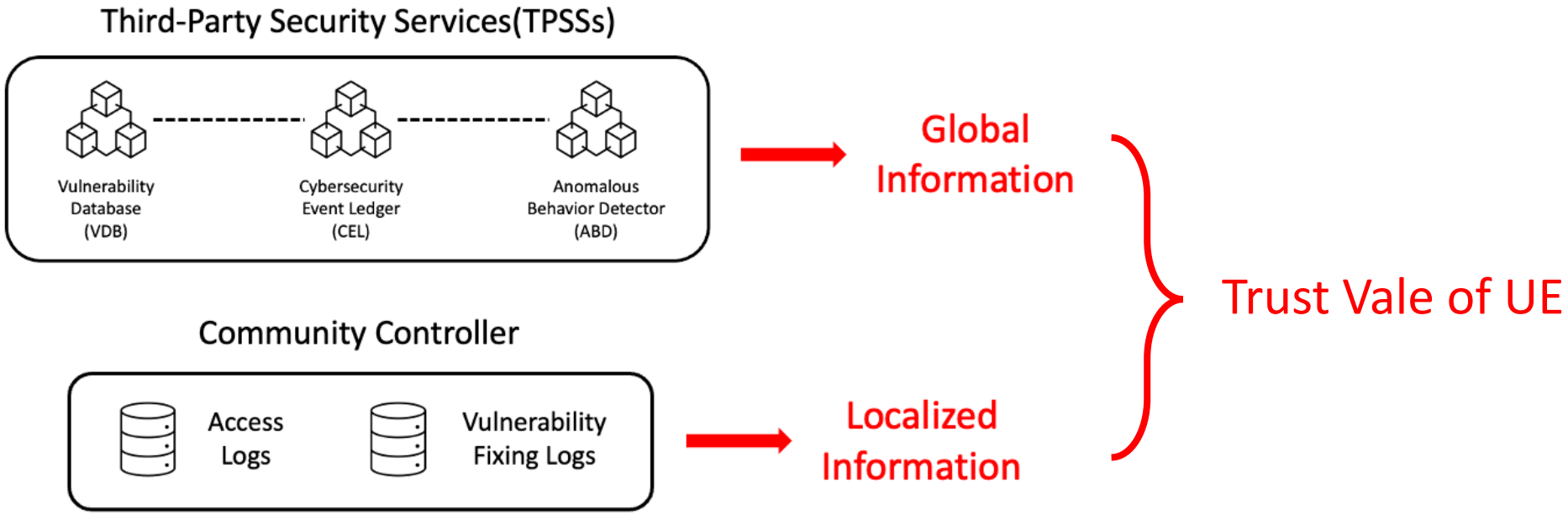
Controller = Community CA



ZTA-6G : A Software-Defined ZTA for 6G Security

> Trust Evaluation System (1)

- In ZTA-6G, **the trust value of the approaching UE** is calculated from the values of the TPSSs and the community controller
- If the trust value exceeds the threshold, it is determined to be **a safe UE** and can access the resource



ZTA-6G : A Software-Defined ZTA for 6G Security

> Trust Evaluation System (2)

Trustworthiness Guarantee

- From UE home community

$$T_{ac} = \alpha T^{C} + (1-\alpha) T^{UE}$$

$$if\ T_{ac} \geq \theta, \textbf{ permit}$$

Trust Value of UE

- *vp = Vulnerability Risk Index*
- *ce = Event Traceability, Forensic Tech.*
- *ab = Abnormal Access Behaviors*

- Trustworthiness of UE

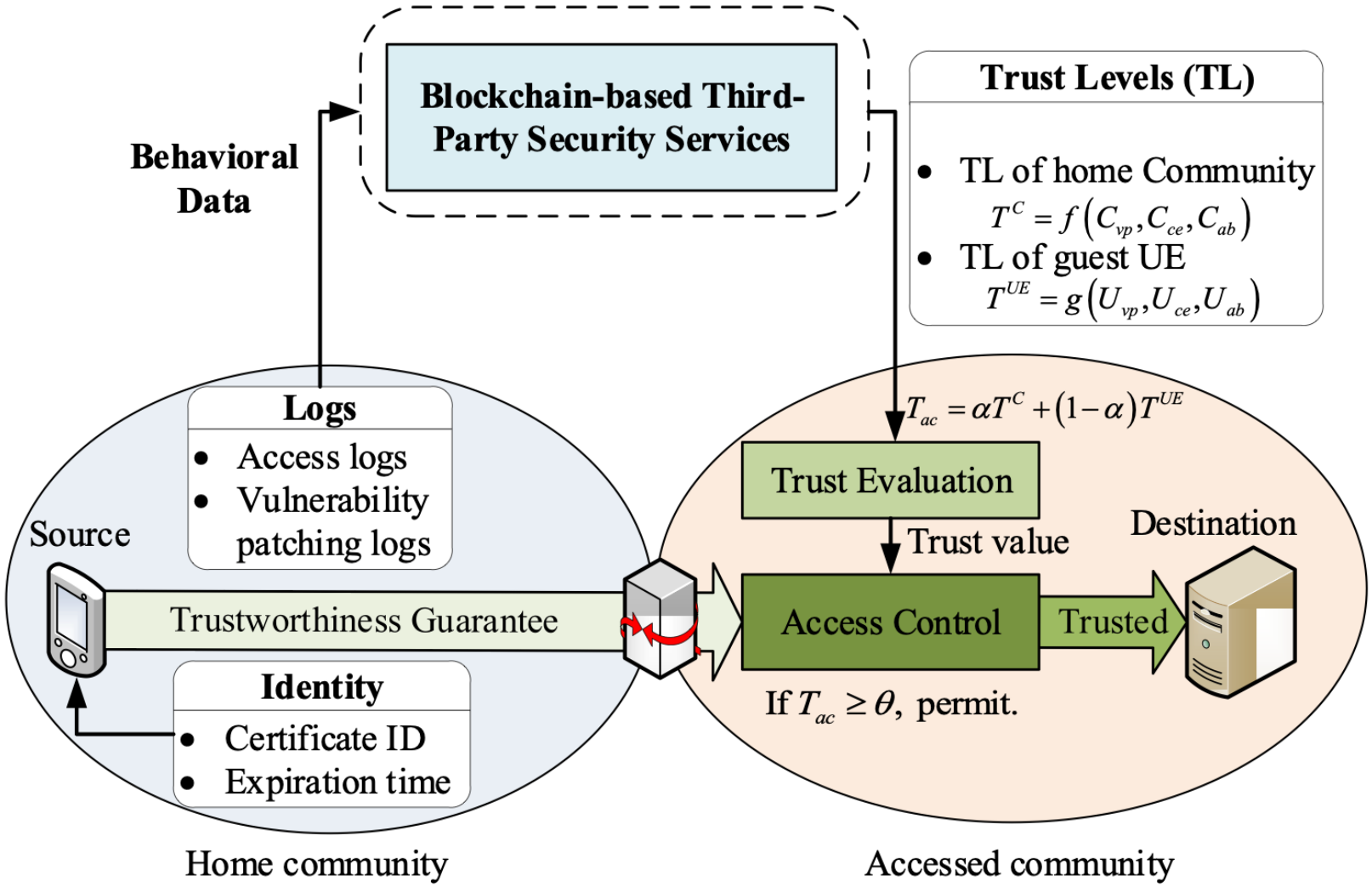
$$T^{UE} = g\left(U_{vp}, U_{ce}, U_{ab}\right)$$

- Trustworthiness of UE Community

$$T^{C} = f\left(C_{vp}, C_{ce}, C_{ab}\right)$$

ZTA-6G : A Software-Defined ZTA for 6G Security

> Trust Evaluation System (3)



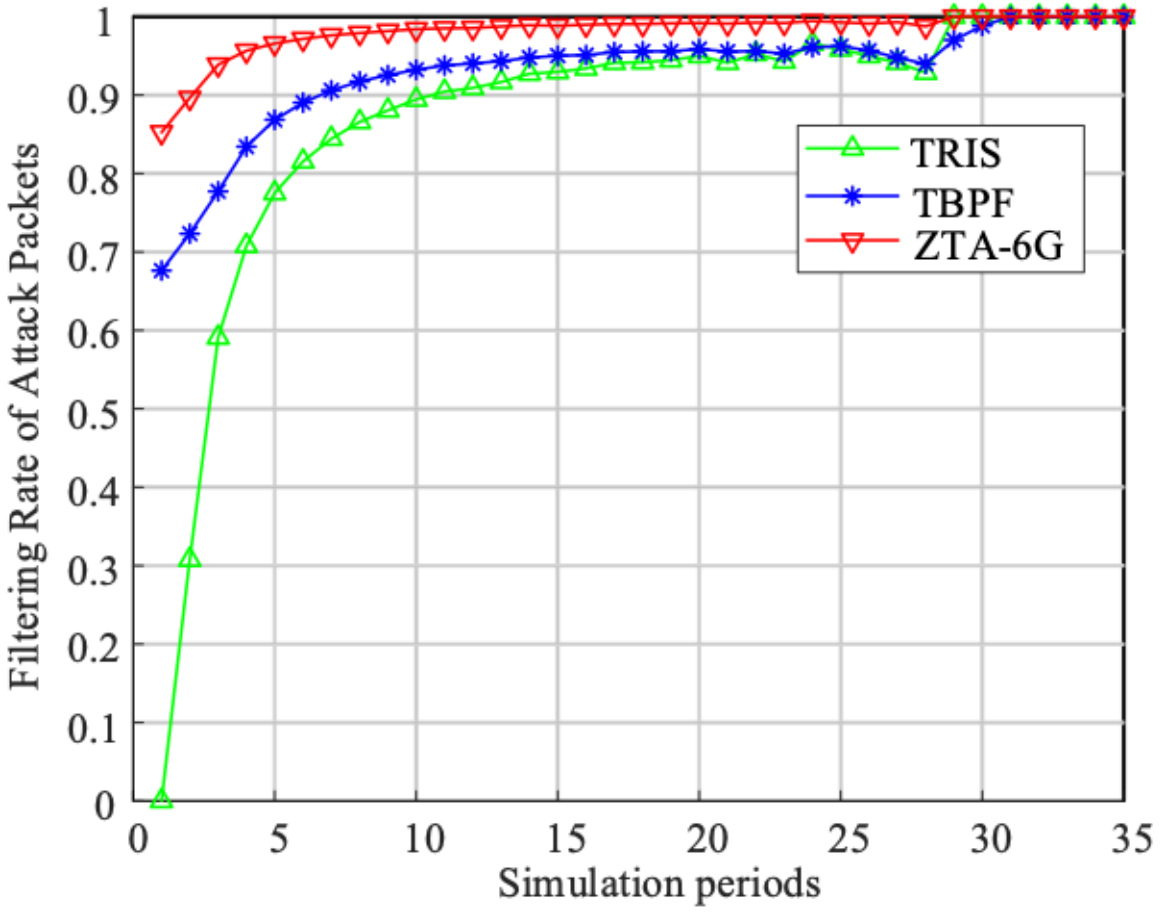
Evaluation

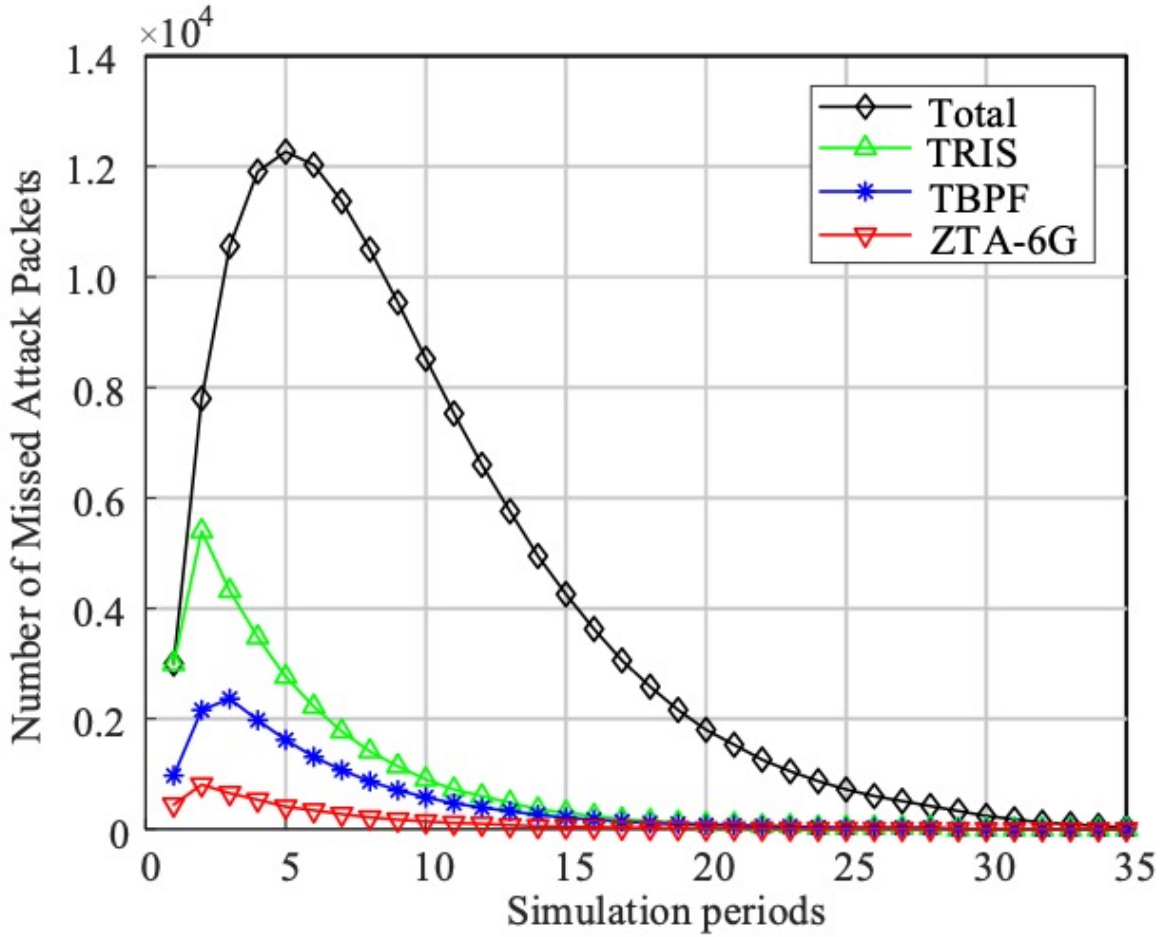
> Environment

- Compare to
  - Trust Based Packet Filtering (TBPF)
  - Transparency for better Internet Security (TRIS)
- Threat scenario includes
  - DDoS attacks, malware, zero-day exploits
- Basic settings
  - 4 communities (A, B, C, D)
  - 1,000 UEs per community
- Malware spreading method
  - Susceptible-infectious-recovered (SIR) model
- Attack measurement
  - Attack starts from A, collects attacked packets at D

Evaluation

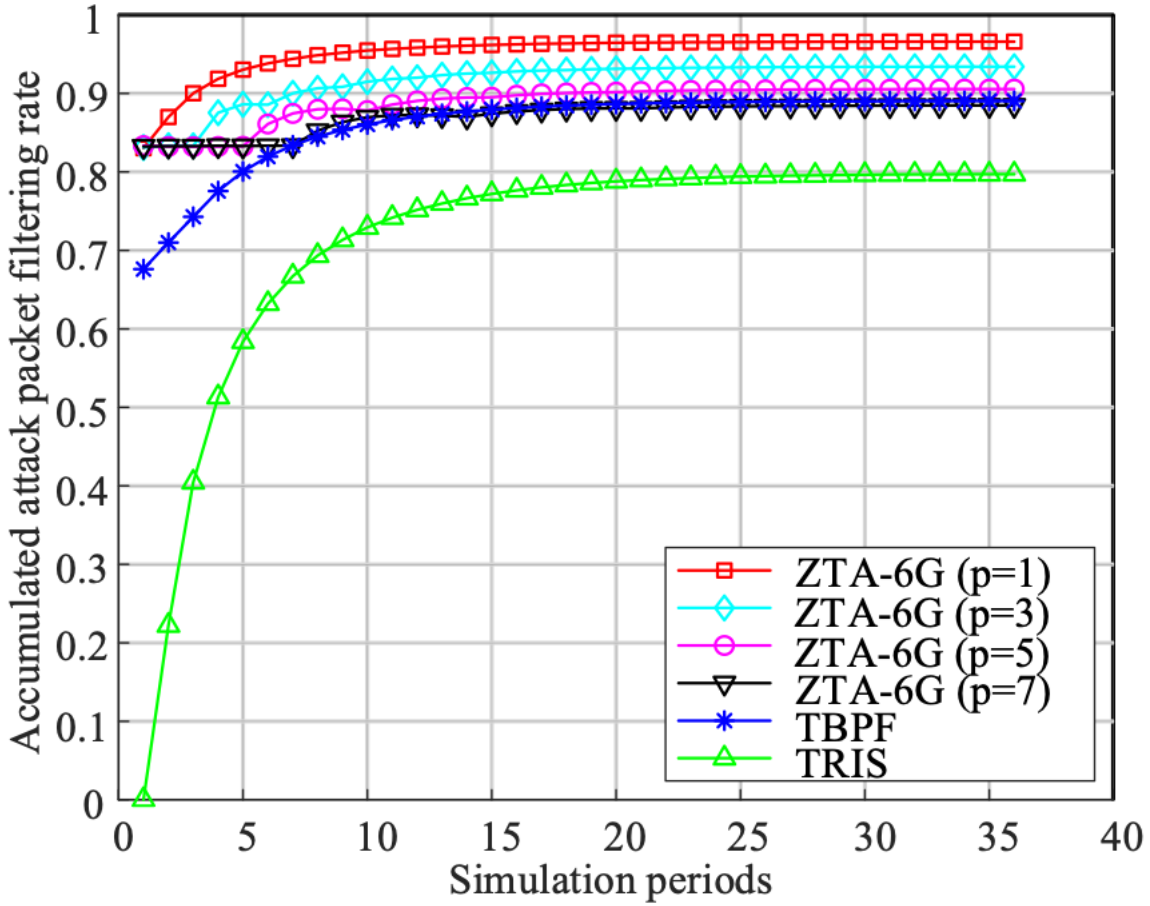
> Filtering Attack Packets and Missing Packets

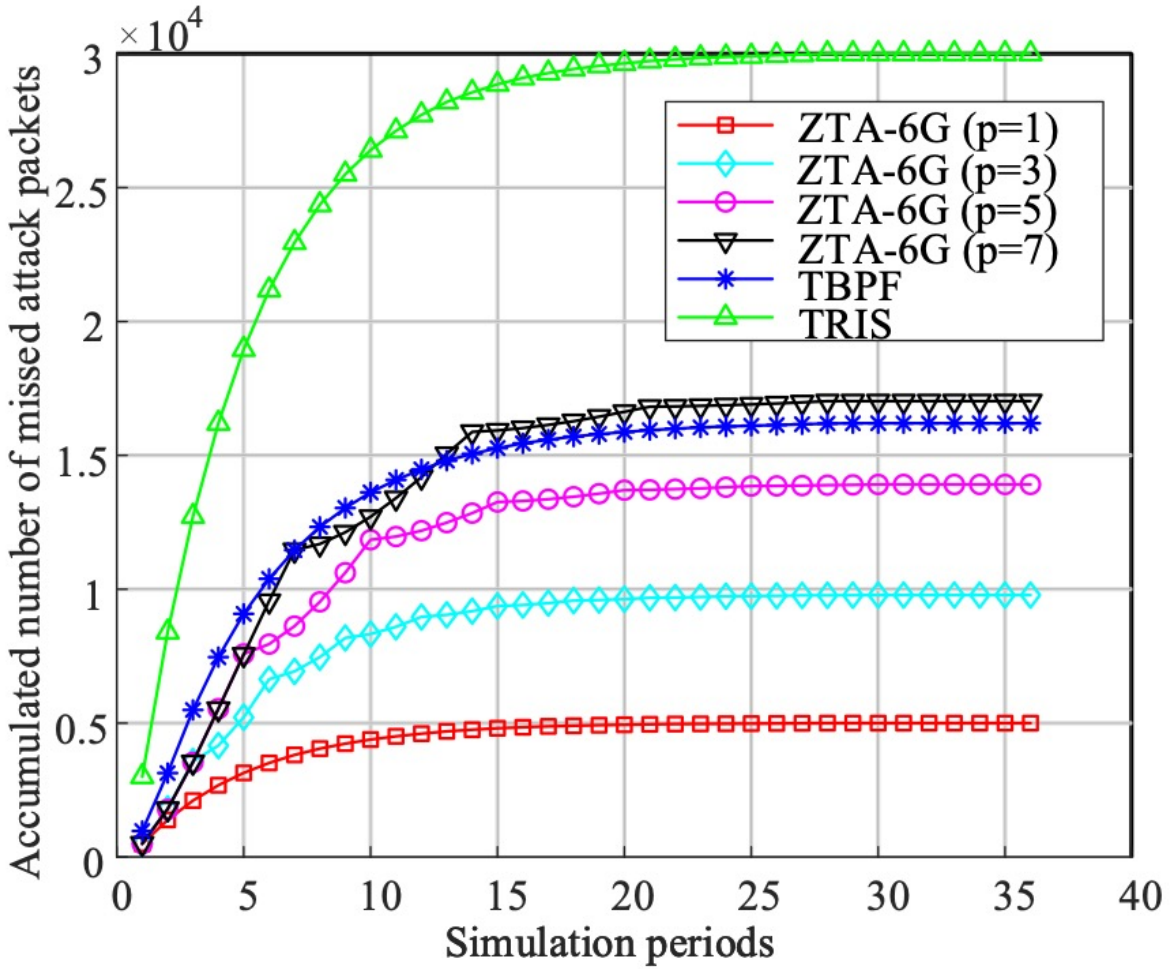




Evaluation

> Robustness





Conclusion

- Zero Trust Architecture (ZTA) is back in the spotlight
- 6G networks present more complex security challenges than traditional networks
- A software-defined ZTA (ZTA-6G) can help address these 6G security challenges
- The ZTA-6G verifies UE by two different way(UE itself + UE community) to increase its trustworthiness

- The authors tried to solve the 6G security challenges with a zero trust architecture, and there were reasonable benefits
- However, there are still open issues such as **delay, mobility issue, post-quantum identity, and cross-chain trust evaluation** that need to be considered.