Zero Trust Architecture for 6G Security

Xu Chen, Wei Feng, Ning Ge, and Yan Zhang

***Abstract*—The upcoming sixth generation (6G) network is expected to be more open and heterogeneous, posing new challenges to conventional security architectures. Traditionally, these architectures rely on the construction of a security perimeter at network boundaries. In this article, we propose a software-defined zero trust architecture (ZTA) for 6G networks, offering a promising approach to establish an elastic and scalable security regime. Our proposed architecture ensures secure access control through adaptive collaborations among control domains, effectively mitigating malicious access behaviors like distributed denial of service (DDoS) attacks, malware spread, and zero-day exploits. We also highlight key design aspects of this architecture and present simulation results from a case study that demonstrate the effectiveness and robustness of ZTA for 6G. Finally, we discuss open issues that warrant further exploration to promote and enhance this novel architecture.**

I. Introduction

Currently, the security challenges associated with the sixth-generation (6G) network are being extensively researched. One of the key challenges lies in ensuring robust security measures. The primary goal of 6G is to establish seamless global connectivity for billions of humans, machines, and devices [1]. However, many of these devices possess weak security capabilities, making them vulnerable to compromise and exploitation for malicious activities. Additionally, the widespread adoption of open-source software technologies introduces security risks stemming from software vulnerabilities. Furthermore, as 6G is an open and integrated network spanning space, air, and ground domains, the integration of multiple control domains with diverse radio access technologies further amplifies the attack surface, owing to their inherent vulnerabilities and security flaws. Conventional security solutions, such as firewalls and intrusion detection systems (IDSs), which rely on perimeter-based defenses, are inadequate in addressing the unique security requirements of 6G [2]. Thus, it has become imperative to develop more elastic security architectures capable of fulfilling the demands of 6G networks.

To address these challenges, we propose a collaborative zero trust architecture (ZTA) specifically designed for 6G networks in this article. Our architecture considers network control domains as communities and harmonizes them to establish robust access control mechanisms for safeguarding their internal network entities. Through adaptive collaborations among the involved control domains, which are maintained by multiple operators, we establish a decentralized network access control regime. To overcome resource limitations within communities, we introduce blockchain-based third-party security services, offering computing power and global information support.

One of the key strengths of our architecture is its ability to dynamically control cross-community access behaviors of user equipment (UE). This dynamic access control effectively prevents the spread of computer viruses, mitigates distributed denial of service (DDoS) attacks, and provides defense against zero-day exploits. Additionally, our architecture strikes a balance between distributed and centralized control, thereby overcoming the scalability limitation of traditional security architectures. This characteristic is particularly advantageous for large-scale and heterogeneous 6G networks.

While our proposed architecture demonstrates significant potential, there are several open issues that require further research. These include system efficiency, mobility management, post-quantum identity schemes, and cross-chain trust evaluations. Addressing these issues will contribute to the successful implementation and deployment of our architecture in practical 6G networks.

II. Challenges in 6G Security

A. *Threat analysis*

4G mobile networks could tackle the problem of spoofing through fake base stations. However, the identities of 4G UEs remain vulnerable to probing by attackers. 5G architecture attempted to address this issue by implementing unified data management and concealed identifiers. However, these security enhancements primarily focused on improved authentication, which remain insufficient in resolving the security challenges posed by 6G networks.

The openness of 6G networks leads to a close integration of access networks and enterprise applications. Consequently, authentication mechanisms become customized to align with the specific access network, making cross-domain security authentication more challenging. Even within a single network domain, traditional authentication and key agreement protocols such as 5G AKA (Authentication and Key Agreement) in mobile networks fail to prevent legitimate but compromised UE from engaging in malicious activities. While Transport Layer Security (TLS), specifically version 1.3, is predominantly used to establish end-to-end secure channels and protect information confidentiality, it does not guarantee the security of communication behavior itself.

In 6G networks, both UE and network entities face numerous threats originating from various technology trends. These threats arise from factors such as network openness, virtualization, containerization, adversarial machine learning, and unauthorized utilization of user information [2]. Given the diversity in these trends, establishing a uniform network-wide defense architecture at the application level becomes challenging.

Alternatively, focusing on the network layer, it becomes evident that most malicious activities are carried out through

X. Chen, W. Feng (corresponding author) and N. Ge are with the Department of Electronic Engineering, Tsinghua University, Beijing, China. X. Chen is also with Naval Research Institute, Beijing, China. Y. Zhang is with the Department of Informatics, University of Oslo, Oslo, Norway.

abnormal access behavior. Consequently, implementing access control at the network layer presents a viable approach to mitigate such threats. Looking ahead, we anticipate the emergence of highly detrimental attacks targeting the network layer in 6G networks, including DDoS attacks, malware spread, and zero-day exploits. Addressing these threats requires robust access control mechanisms and proactive security measures at the network layer.

- *DDoS attacks*. DDoS attacks pose a significant threat as they can inflict damage solely through access behaviors. In the context of 6G networks, the severity of DDoS attacks is expected to increase significantly due to the exponential growth in the number of potential bot devices. Among the susceptible targets, edge servers and UEs are particularly vulnerable, primarily due to their limited mitigation capabilities.
- *Malware*. Malware represents a malicious code that attackers inject into victims through access behavior. It encompasses various forms, including computer viruses, worms, Trojan horses, ransomware, and rootkits. Malware can cause significant damage to the integrity, confidentiality, and availability of network resources in 6G networks.
- *Zero-day exploits*. Zero-day attackers leverage software vulnerabilities to inflict damage through network access. In 6G, the adoption of open-source software in network entities increases the risk of zero-day exploits. Attackers can exploit zero-day vulnerabilities to disrupt network functions and compromise the security of 6G networks.

B. Security challenges

We summarize new security challenges for 6G as follows.

- Ultra large scale. Given the ultra-large-scale nature of 6G networks, scalability becomes a critical factor when designing the security architecture. Traditional high-complexity architectures may not be cost-effective or even feasible for such a scale.
- Heterogeneity. In 6G networks, the presence of heterogeneous networks managed by multiple operators introduces complexities in management and signaling systems. Collaboration among control domains with diverse management modes is essential for 6G security architectures. The heterogeneity of UEs also poses challenges for security architecture design. A centralized architecture may fail to meet these requirements.
- Openness. Incorporating the Open Radio Access Network (O-RAN) in 6G introduces new forward interfaces and network entities from multiple vendors. This openness brings challenges to the architecture. The increased complexity and integration difficulty can lead to system fragility, additional points of failure, and heightened security risks.
- Autonomous interactivity. Machine-to-machine (M2M) communication is expected to be a prominent application scenario in 6G networks. The ubiquitous collaboration requirements necessitate interactivity among intelligent devices. These interactions primarily occur autonomously, without human supervision. As a result, the security architecture needs to closely monitor access behavior in a fine-grained manner to mitigate the risks associated with such interactions.

C. ZTA and its limitations in 6G

ZTA, with its core principle of "never trust and always verify," was introduced to dynamically protect digital resources in local networks[3]. This approach becomes particularly relevant as traditional network boundaries become blurred, making dynamic access control crucial for avoiding security issues. Several enterprises have undertaken technical research and engineering practices in this area. Gartner initially proposed the Adaptive Security Architecture (ASA) in 2014, which has since evolved into the Zero Trust Network Access (ZTNA) concept. Google also developed the BeyondCorp security model to meet its internal network security governance requirements starting in 2014. According to a report that surveyed over 400 cybersecurity decision-makers, 72% of organizations planned to assess or implement zero trust capabilities before 2021. Furthermore, Gartner predicted that by 2023, 60% of these enterprises would transition to ZTNA solutions [4]. These statistics highlight the increasing demand towards ZTA in an ever-changing threat landscape.

However, existing ZTAs face significant challenges in addressing the unique security concerns of 6G networks. Firstly, current ZTAs primarily rely on fine-grained access control strategies to safeguard all data resources and computing services [5]. They may struggle to effectively handle the scale and complexity introduced by the ultra large-scale nature of 6G networks. Secondly, existing ZTAs are predominantly designed for single network domains that utilize a logically centralized controller. This restricts their applicability to 6G networks with decentralized management architectures. Thirdly, end-to-end encryption is a fundamental requirement in existing ZTAs [3]. However, the resource limitations make it challenging for Internet of Things (IoT) in 6G to fulfill the demanding encryption requirements. Lastly, while existing ZTAs primarily aim to prevent data breaches and mitigate internal lateral movement, they may not adequately address the specific security requirements of 6G networks, such as effectively countering flooding attacks.

Although the newly emerged software-defined perimeter (SDP) technology [6] has extended the concept of ZTA to the network and transport layers, there are still few considerations of other challenges. The tailoring of ZTA for 6G large-scale network security has become an important issue. The authors of [7] have made significant attempts in this respect, but their focus primarily revolves around the detection accuracy and cost of attacks rather than the construction of trust systems. Furthermore, their proposed architecture is centralized, which may present scalability concerns in the context of 6G networks. This article aims to construct a comprehensive zero-trust system based on 6G networks to fill this gap.

III. Zero Trust Architecture for 6G

We introduce the key design aspects of ZTA for 6G, which include the distributed security architecture, decentralized identity management, and trust evaluation system.

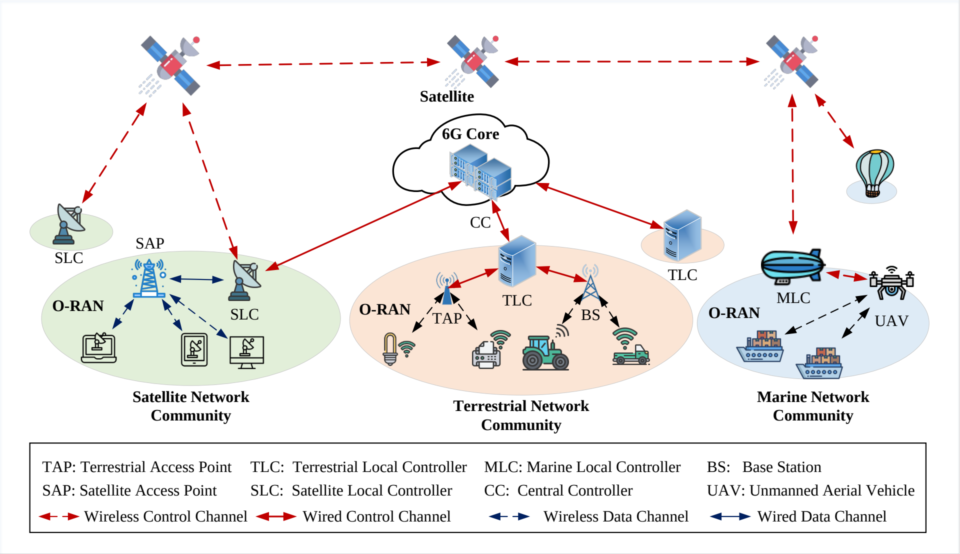
Satellite
6G Core
CC
TLC
SLC
SAP
O-RAN
SLC
Satellite Network Community
O-RAN
TAP
TLC
BS
Terrestrial Network Community
O-RAN
MLC
UAV
Marine Network Community
TAP: Terrestrial Access Point
SAP: Satellite Access Point
TLC: Terrestrial Local Controller
SLC: Satellite Local Controller
MLC: Marine Local Controller
CC: Central Controller
BS: Base Station
UAV: Unmanned Aerial Vehicle
Wireless Control Channel
Wired Control Channel
Wireless Data Channel
Wired Data Channel

Fig. 1. 6G network architecture. The network managed by each local SDN controller constitutes a community.

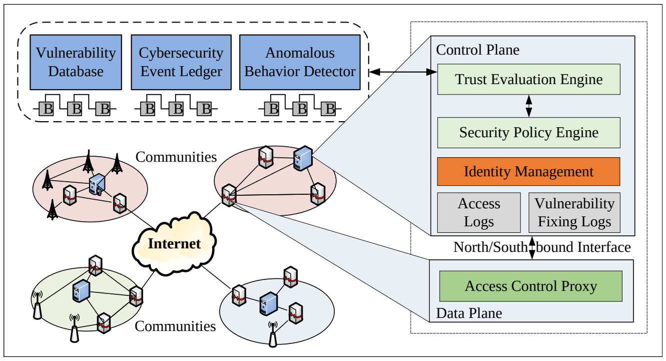

Fig. 2. Access control framework based on communities in ZTA.

A. Distributed security architecture

As 6G is an integrated network operated by many different operators, the SDN-based control architecture should be distributed and adaptive. For example, in remote areas, distributed control architectures are suitable for efficiency considerations, whereas in urban areas, a hierarchical control architecture is required for scalability [8]. To ensure its deployability, the ZTA for 6G must be adapted to the hybrid control architecture.

As shown in Fig. 1, a community is a subnetwork managed by a local SDN controller in 6G. In 6G cloud native architecture, the controller is usually deployed on cloud platforms. The security function of communities in ZTA is to perform access control at border switches to protect the internal equipment from external threats. In ZTA, communities play a role similar to that of home networks in LTE/5G mobile networks. Just as a UE can roam between different home networks in mobile networks, a UE can move between different communities. However, the access authentication for the UE is still managed by its home community until it joins a new community.

The access control framework for the communities is shown in Fig. 2. The access control proxy on data plane forwards guest UE's access requests to the control plane through the northbound interfaces for processing. It also implements the access control decisions returned by the control plane. The control plane consists of three modules: an identity management module, a security policy engine (SPE), and a trust evaluation engine (TEE). The SPE formulates access control strategies for specific access requests, supported by the TEE. The TEE evaluates the trustworthiness of visitors based on third-party trust assessment results. The identity management module handles identity verification and certificate approval for all UEs in the community. Additionally, two databases are utilized to store the vulnerability fixing logs and access logs of UEs.

To address the limitations of communities in terms of resources and information, we introduce third-party security services (TPSSs) based on public blockchains. These services include the vulnerability database (VDB), cybersecurity event ledger (CEL), and anomalous behavior detector (ABD). The VDB offers risk assessment services to the trust evaluation engine (TEE) in the accessed community. It analyzes recent vulnerability releases and vulnerability fixing logs associated with the guest UE to determine the risk levels of vulnerable UEs based on the severity and potential harm of unfixed vulnerabilities. The CEL verifies if the guest UE has interacted with a virus-infected UE or accessed victims during recent attack events. This is accomplished by searching records obtained through victim reports and network forensics. The ABD employs artificial intelligence techniques to conduct behavior analysis and identify potential security risks based on the guest UE's recent access behaviors. The TEE in the accessed community usually initiates the behavior analysis request, and the guest UE's home community provides historical access logs upon demand. We introduce blockchain technology to ensure the data integrity and availability for TPSSs. Note that the blockchain is employed as a distributed ledger, and its transaction efficiency issues do not restrict the response time of the security architecture.

It is worth noting that the functional scope of TPSSs is not limited to the network layer. In fact, application-layer vulnerabilities, attack events, and anomalous behaviors can be incorporated in TPSSs for evaluation, making them bridges to a cross-layer security system. In addition, the introduction of TPSSs opens up secure interfaces and potential collaborative mechanisms with existing application-layer security architectures.

When a UE initiates an access request, the home community evaluates and blocks the request if the UE is potentially malicious. After self-evaluation, the UE's digital identity and related security certifications are submitted to the border switch of the accessed community for evaluation. The border switch maintains an access control list based on its flow table, and activates the access control mechanism for new access requests. For roaming UEs, the self-evaluation process are also conducted by the home community through the home network control mechanism. This approach aligns with the roaming management mechanism implemented in 5G networks.

Within the accessed community, access control is conducted collaboratively with the assistance of TPSSs. When necessary, the SPE sends assessment requests to the TPSS upon receiving an access request from the border switch. The TPSS evaluates the trust level associated with the request and communicates the results back to the TEE. The TEE utilizes the feedback from the TPSS to calculate the trust value, which is then relayed to the SPE. The SPE, in turn, makes access control decisions based on the security control policies of the community and the trust value received from the TEE. This community-based security architecture is specifically designed to effectively adapt to the large scale and heterogeneity of 6G networks.

B. Decentralized identity management

Identity is the most important infrastructure in ZTAs, and it determines the home community of a UE. In 6G, it is very difficult to establish and maintain a unified identity system due to more diversified network equipment suppliers, network operators and heterogeneous network structures. Traditional identity authentication schemes based on data certificates cannot satisfy the requirements of access control in 6G. In centralized identity management schemes, a unified certification authority (CA) issues certificates for all requesting UE, which restricts the scalability of the entire system. If multiple CAs are employed, the problem of mutual trust cannot be resolved. In totally distributed identity management schemes, if the service provider (e.g., the cloud servers) issues a digital certificate to each potential visitor, a UE has to retain too many digital certificates. Decentralized identifiers are of great importance for ZTA in 6G networks [9].

In fact, a unique identity across the entire network is not only unnecessary but also leads to privacy issues. Digital twin technologies have provided us with a distributed identity mechanism based on blockchain. However, such a unified identity system requires additional privacy protection measures for user data. The complex calculations involved limit the efficiency and scalability of access control in 6G enabled IoTs. To this end, we propose a decentralized identity management scheme based on digital certificates. In this scheme, the certificate can be generated by either the UE or the home communities. The local controller of each community is the only CA responsible for the authentication of digital certificates. The community-based identity management scheme is illustrated in Fig. 3.

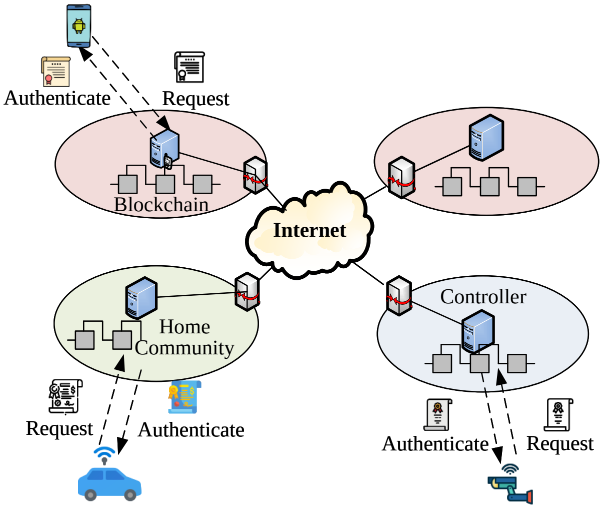

Fig. 3. Community-based decentralized identity authentication.

- Certificate generation. The digital certificate can be autonomously generated either by the UE, or the local controller if the UE is weak. The certificate format can be customized by the community as long as the proof of identity, UE type, operating system (OS) version, and other related information are specified. The generated certificate is encrypted and submitted to the controller for approval. This scheme can effectively alleviate the controller's workload.
- Certificate registration. The local controller decrypts the submitted certificate and verifies relevant information. If successful, a unique certificate ID, a validity period and other restrictions are assigned. After signing with the controller's private key, the certificate is returned to the applicant UE as a legal identifier. The registration information of certificates can be stored centrally on the controller or distributed on the community's private blockchain according to the security requirements.
- Certificate updating. If a UE needs to update its digital certificate, it updates the relevant content of the certificate, such as the public key, and performs the certificate generation and registration process again. The controller can use the original certificate ID. It suffices to review, resign, and return it to its holder.
- Certificate revocation. When a UE changes its home community or in other necessary conditions, the digital identity can be revoked. During certificate revocations, the controller cancels the certificate ID from the identity database. The controller can also implement certificate revocation by setting a short validity period.

The advantage of introducing blockchain is to ensure the integrity and confidentiality of digital certificates within the

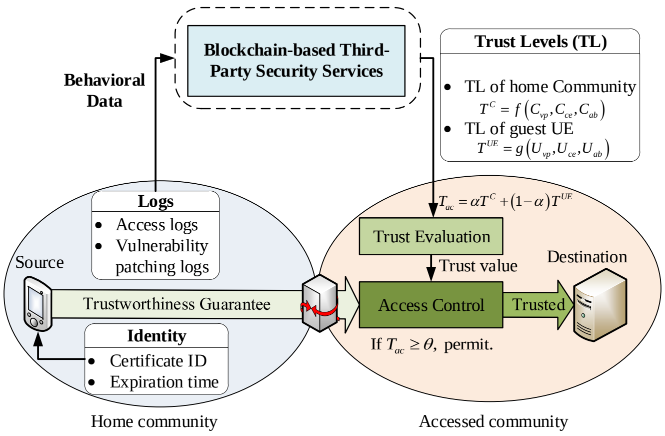
Blockchain-based Third-Party Security Services
Behavioral Data
Trust Levels (TL)
TL of home Community
$T^C = f\left(C_{vp}, C_{ce}, C_{ab}\right)$
TL of guest UE
$T^{UE} = g\left(U_{vp}, U_{ce}, U_{ab}\right)$
Logs
Access logs
Vulnerability patching logs
$T_{ac} = \alpha T^C + (1-\alpha) T^{UE}$
Trust Evaluation
Trust value
Source
Destination
Trustworthiness Guarantee
Access Control
Trusted
Identity
Certificate ID
Expiration time
If $T_{ac} \geq \theta$, permit.
Home community
Accessed community

Fig. 4. The trust evaluation process employed in the proposed ZTA.

community, avoiding the risk of a single point of failure caused by a centralized storage. The blockchain can be deployed on some or all of the computing nodes such as edge servers in the community, and the implementation details have been specifically studied in the literature [10]. Based on this identity authentication scheme, UE identification can be achieved through hierarchical retrieval by introducing community identifiers (IDs). Specifically, an integrated UE identity consists of three parts: an autonomous system number (ASN), community ID, and certificate ID. The ASN is unique within the entire 6G network. The community ID needs to be unique within the AS to which it belongs, and the certificate ID of a UE needs to be unique within the community in which it resides. The ASN and community ID should be attached as identification elements in cross-domain access. Because only the home community can resolve the certificate ID and it can be dynamically changed, the privacy of the UE identity can be preserved. This design not only meets the access control requirements of diversified UE in 6G but also increases the elasticity and scalability of the identity management scheme.

C. Trust evaluation system

Trust evaluation is the process of quantifying trust values based on the attributes that affect trust. Trust in communication networks comes from the observation of the historical behaviors and recommendations of trusted third parties [11]. In the proposed ZTA, the trust evaluation system operates as illustrated in Fig. 4. The trustworthiness of a guest UE is initially ensured by its home community through processes such as identity authentication and self-evaluation. Subsequently, the accessed community assesses the trustworthiness of the guest UE by utilizing the trust attributes provided by the TPSSs. The TPSSs, such as the VBE, CEL and ABD, evaluate specific security characteristics of the guest UE, which can be denoted as U_{vp}, U_{ce} and U_{ab}. These trust attributes are then utilized in the calculation of the guest UE's overall trust level (T^{UE}) through a trust evaluation function denoted as $g(\cdot)$. While this article primarily focuses on the general architecture of the trust system, a comprehensive discussion of the specific trust evaluation function is beyond its scope. Detailed implementations and considerations can be found in related works such as [10] and [11]. For instance, the work presented in [10] introduces a reputation-based consensus process designed specifically for blockchain networks, which can serve as a reference for implementing the trust evaluation process in our ZTA.

The information used by the TPSSs for trust evaluation, including identity and behavioral data, is dependent on the trustworthiness of the home community. If the home community maliciously provides false UE identity information or forged logs, it seriously undermines the validity of the trust evaluation results and affects the security performance of the access control framework. Therefore, to prevent attackers from manipulating community controllers to engage in large-scale malicious behaviors, the trustworthiness evaluation mechanism of communities must be established to solidify the trust root of the whole ZTA.

In our ZTA, we consider the community as a single entity, and it is responsible for vulnerability patching, supplying necessary data to the TPSSs and conducting self-evaluations of UE for cross-domain access. These three types of behaviors can be evaluated separately over a specific timeframe and then we synthesize the results to derive a comprehensive trust value for the community.

To this end, we introduce TPSSs as supervisors to evaluate the trustworthiness of each community in terms of vulnerability risk, threat level and behavior abnormality. VDB maintains a community vulnerability risk index C_{vp} through periodic or random scanning to evaluate the timeliness of vulnerability patching in the community, and impose indicator penalties on fraud and deception. CEL employs event traceability and network forensic techniques to collect statistics on the distribution of attackers, virus sources, and bots to form a threat level evaluation index C_{ce} of communities. ABD performs statistical analysis on the frequency of abnormal access behaviors and other characteristics to generate a community behavior abnormality index C_{ab}. The community's trust level T^C can be formulated by a user-defined function $f(\cdot)$ of these three indices. The trust value of the guest UE (i.e., T_{ac}) can be obtained by the weighted sum of UE trust level T^{UE} and community trust level T^C. The weighted coefficient α is set by the administrator to adjust the proportion of the community trust level in the comprehensive trust value. Then, the TEE can make access decisions accordingly. If the UE's trust value exceeds the required threshold θ defined by the SPE, the access request is permitted. Otherwise, it is denied. By incorporating the trust level of the home community as a trust attribute of the guest UE, the approval probability of their access requests can be affected.

By introducing community-level trust as a reference factor in access control, community controllers can be effectively encouraged to focus on improving security performance to ensure the access authority of their customer UE. Even though data fraud cannot be completely eliminated, such behaviors can be effectively punished, thereby significantly reducing the occurrence probability of dishonest communities. Therefore, the foundation of the entire trust system can be consolidated to adapt to the openness of 6G.

This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2023.3326356

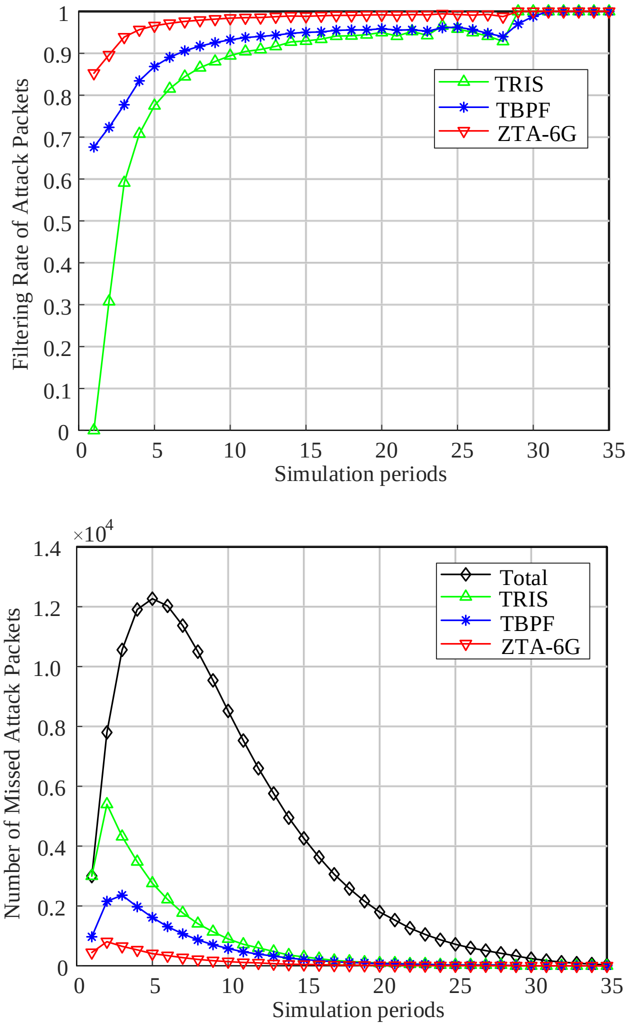

Fig. 5. Effectiveness of different security architectures in defending against non-spoofing DDoS attacks. The subfigure above illustrates the filtering rates of attack packets under different security architectures, and the subfigure below shows the number of missed attack packets.

IV. Numerical Results

To verify the effectiveness of the proposed ZTA for 6G, that is, ZTA-6G, we compare it with two security architectures, Trust Based Packet Filtering (TBPF) [12] and Transparency for better Internet Security (TRIS) [13]. TBPF was developed to enable collaboration among multiple IDSs based on the trust evaluation of nodes and IP addresses. TRIS was proposed based on profound insights into DDoS attack defense, which can be applied to the security defense of the entire network. We chose a composite threat scenario involving DDoS attacks, malware, and zero-day exploits. The experiment settings are as follows.

- *Basic settings*. We establish a network consisting of four communities, namely A, B, C and D, with 1,000 UEs each. Backbone links are established between A-B, A-C, B-D, and C-D. Although remotely manipulating bots across communities can be prevented in ZTA-6G, bot-herders can still manipulate infected UEs within the same community to launch attacks. Multiple attackers can launch zero-day DDoS attacks through cross-community coordination. Before the attack is launched, we simulate a normal communication process lasting for 100 s with a cross-domain access probability of 0.1 at a rate of 5 packets per second (pps).
- *Malware spreading.* We adopt the susceptible-infectious-recovered (SIR) model [14] to simulate the spread of worms in communities. The infection and fixing rates of the vulnerability are both set to 0.2. Initially, each community starts with 100 infected UE instances. The simulation progresses in periods of 1 second each, repeating until all vulnerable UEs are fixed.
- *Attack scenario.* Since ZTA-6G is inherently resistant to IP spoofing, we evaluate the effectiveness of defense against non-spoofing attacks. The infected UEs in B and C first attack a victim in A, then the infected UEs in A, B, and C jointly attack the victim in D to simulate a DDoS attack. The attack intensity is set at 10 pps.
- *Trust evaluation.* For ZTA-6G, we adopt the same trust evaluation method as for TBPF [12], which established a Bayesian inference model to determine the probability that the next arriving packet is normal. We set the threshold of the trust value in TBPF to 0.75, as suggested by the authors.

We collect the received attack packets at the victim side in community D to evaluate the defense performance of each architecture. The average results of 100 random simulations are shown in Fig. 5.

As shown in Fig. 5, as the simulation process proceeds, the defense effects of the three architectures generally improve, wherein ZTA-6G always performs the best. TRIS cannot defend against the first attack of malicious UE, so its defense effect is the worst at the very beginning. The performance of TBPF is better. ZTA-6G filters out the packets from UEs with malicious behaviors in the source community by self-evaluation and re-evaluates the trustworthiness of vulnerable UEs in the destination community. Thus, it maintains the highest filtering rate of attack packets. Therefore, the number of missed attack packets is minimal (as shown in the subfigure below).

To verify the robustness of the ZTA-6G, we set different validity periods for the trust evaluation results instead of evaluating the trustworthiness of every access request. For the evaluation results of UEs within the validity period, ZTA-6G directly approves their access requests. Some UEs become bots owing to virus infection during this period, resulting in the degradation of security performance in terms of the accumulative filtering rate in non-spoofing DDoS attacks. We set the validity period to 1, 3, 5, and 7 s to verify the changes in the accumulated filtering rate of the attack packets and the number of missed attack packets by ZTA-6G. The average results of 100 random simulations are shown in Fig. 6.

As the validity period increases, the accumulative filtering rate of attack packets shows a downward trend, but the rate of decline slows down. Implementing trust evaluation every second ($p = 1$) performs the best, and its time cost is the highest. For $p > 1$, the accumulative filtering rate

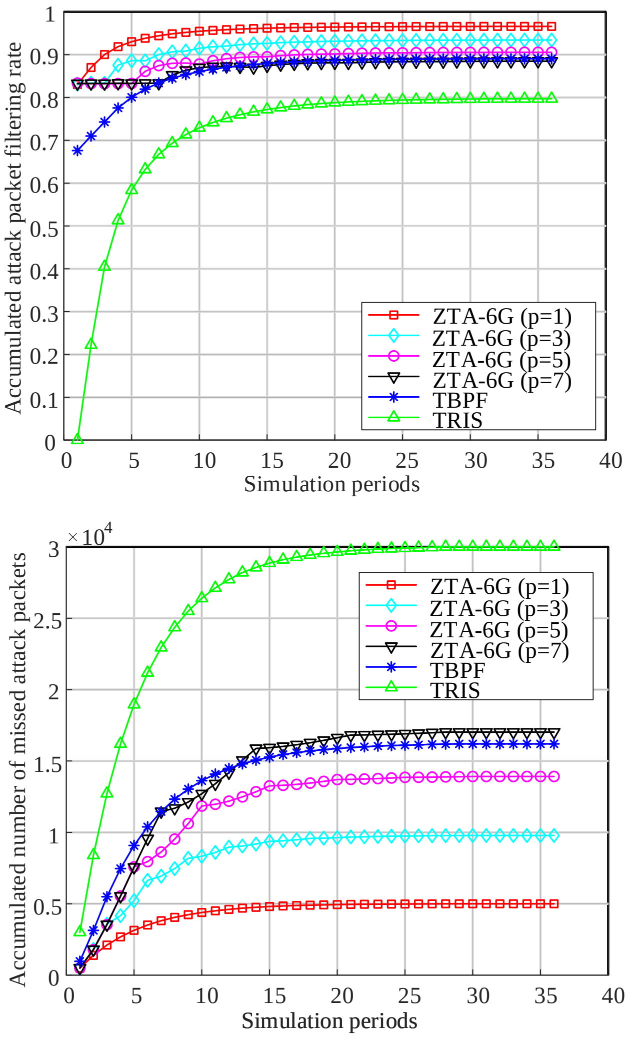

Fig. 6. Robustness of the proposed ZTA in different validity periods of the trust evaluation results. The subfigure above shows the accumulated filtering rates of attack packets by each method, and the subfigure below shows the accumulated number of missed attack packets.

curves are wavy. This is because, after each re-evaluation, the effectiveness of the evaluation results declines over time. For $p = 3$ and $p = 5$, ZTA-6G performs much better than TRIS and TBPF. The accumulated detection rates are both higher than 90%. Even if we re-evaluate the UE's trust value once every 7 s, the filtering rates of attack packets can still be much better than TRIS and are almost as good as TBPF. These results demonstrate the robustness of ZTA-6G. In addition, this also shows that it is feasible to sacrifice a small part of the security performance to obtain a significant improvement in time efficiency according to the safety requirements in applications.

Next, we evaluate the cost of implementing a private blockchain for identity management. In general, the transaction information for certificate registration encompasses UE identity (up to 128 bits), UE type (up to 128 bits), OS details (up to 256 bits), certificate ID (typically of 256 bits), public key (2048 bits with the RSA2048 algorithm), and the validity period (comprising activation and expiration, totaling 128 bits). Thus, the data length is less than 2944 bits on aggregate. Besides, certificate updating involves solely UE identity, public key, and validity period, resulting in a data length below 2304 bits. Consequently, the data length for each transaction remains within the confines of 3 kilobytes.

In our simulations, registering or updating all UE certificates in a community requires 1000 transactions. Assuming an average of 20 transactions per block, a total of 50 blocks are needed to store these transactions. Each block encompasses additional data including the block header (640 bits), block size (32 bits), and transaction count (16 bits), contributing to a block size ranging from 5.7 to 7.2 kilobytes. Consequently, the storage overhead for a blockchain node ranges from 0.28 to 0.36 megabytes. Given the enduring stability of certificate information, such storage overhead is acceptable over the long term.

We assume that the private blockchain employs the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, which requires a communication complexity of $O(n^2)$. In a consensus network with 20 nodes, the amount of data transferred to generate a block does not exceed 2.81 megabytes. Considering that the number of computing nodes in a private blockchain is adjustable and usually small, this level of communication cost is well within the capacity of the internal network in a community.

V. Open Issues

To facilitate the implementation of ZTA-6G, there are several open issues to be further studied.

A. *System efficiency*

In ZTA-6G, the delay associated with the trust evaluation process can hinder its application in delay-sensitive services. To mitigate this delay, several approaches can be considered. Content distribution technologies can be used to deploy TPSSs so that communities can access their services nearby. The on-demand extraction of behavioral logs from communities can be replaced by periodic active synchronization to reduce the transmission delay. The behavior analysis algorithm can focus only on the correlation analysis of incremental data to improve processing speed. In a nutshell, improving the system efficiency is a complex problem that requires further research.

B. *Mobility management*

In ZTA-6G, identities, behavioral data, and vulnerability fixing information of UEs are stored and managed based on communities. As a UE moves, its home community may change. Additionally, the movement of network entities like satellites and drones can result in changes in management domains. To ensure timely access control within ZTA, it is crucial to address the handover management problem, particularly for delay-sensitive services. One potential solution involves leveraging artificial intelligence (AI) techniques based on UE mobile pattern prediction.

C. Post-quantum identity

With the anticipated maturity of quantum computing in the 6G era, its remarkable computing power has the potential to revolutionize cryptography and render traditional certificate-based digital identities less secure. To support the operation of our ZTA, it is crucial to explore new distributed identity mechanisms that can withstand brute force cracking facilitated by quantum computing while maintaining robust security performance. One potential candidate is blockchain-based solutions. However, deploying and applying them on weak UEs pose significant challenges.

D. Cross-chain trust evaluations

In our proposed ZTA, we make the assumption that historical cybersecurity information can be shared globally, enabling community controllers to access TPSSs based on a unified public blockchain. However, as we look towards the future metaverse, access control within distinct submetaverses may necessitate the involvement of TPSSs from diverse and heterogeneous blockchains [15]. This introduces a new challenge of cross-chain trust evaluation. Efficient mechanisms for cross-chain security information sharing and trust evaluation need to be further explored and studied.

VI. Conclusions

To address the evolving security needs of 6G networks, we have designed a software-defined ZTA that enables collaborative defense against network threats. Our architecture incorporates sophisticated access control for guest UE through trust assessment from TPSSs. Distributed identity management is achieved using a newly developed digital certificate system. The architecture establishes a trust evaluation system with TPSSs as supervisors, solidifying the trust roots. We have verified the effectiveness and robustness of our proposed ZTA through simulations of worm-spreading and zero-day DDoS attacks. The results confirm the efficacy of our architecture in mitigating these threats.

Acknowledgments

This work was supported in part by the National Key R&D Program of China (Grant No. 2020YFA0711301), and in part by the National Natural Science Foundation of China (Grant No. 62201605, 62341110, U22A2002).

References

[1] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G Embraces Satellites for 6G Ubiquitous IoT: Basic Models for Integrated Satellite Terrestrial Networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14 399–14 417, 2021.

[2] D. Je, J. Jung, and S. Choi, "Toward 6G Security: Technology Trends, Threats, and Solutions," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 64–71, 2021.

[3] E. Gilman and D. Barth, *Zero Trust Networks*, 1st ed. Sebastopol, CA: O'Reilly Media, Inc., July 2017.

[4] H. Schulze, "Zero Trust Progress Report," Cybersecurity Insiders, Tech. Rep., 2020. [Online]. Available: https://www.cybersecurity-insiders.com/portfolio/2020-zero-trust-progress-report-pulse-secure/

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Tech. Rep., 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[6] A. Moubayed, A. Refaey, and A. Shami, "Software-Defined Perimeter (SDP): State of the Art Secure Solution for Modern Networks," *IEEE Network*, vol. 33, no. 5, pp. 226–233, 2019.

[7] H. Sedjelmaci and N. Ansari, "Zero Trust Architecture Empowered Attack Detection Framework to Secure 6G Edge Computing," *IEEE Network*, pp. 1–13, 2023.

[8] X. Li, W. Feng, J. Wang, Y. Chen, N. Ge, and C.-X. Wang, "Enabling 5G on the Ocean: A Hybrid Satellite-UAV-Terrestrial Network Solution," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 116–121, 2020.

[9] S. R. Garzon, H. Yildiz, and A. Küpper, "Decentralized Identifiers and Self-Sovereign Identity in 6G," *IEEE Network*, vol. 36, no. 4, pp. 142–148, 2022.

[10] Y. Wang, Z. Su, K. Zhang, and A. Benslimane, "Challenges and Solutions in Autonomous Driving: A Blockchain Approach," *IEEE Network*, vol. 34, no. 4, pp. 218–226, 2020.

[11] A. Das and M. M. Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 261–274, 2012.

[12] W. Meng, W. Li, and L. F. Kwok, "Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments," *IEEE Transactions on Network and Service Management*, vol. 14, no. 1, pp. 233–245, 2017.

[13] C. Pappas, T. Lee, R. M. Reischuk, P. Szalachowski, and A. Perrig, "Network Transparency for Better Internet Security," *IEEE/ACM Transactions on Networking*, vol. 27, no. 5, pp. 2028–2042, 2019.

[14] W. K. Chai, "Modelling Spreading Process Induced by Agent Mobility in Complex Networks," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 4, pp. 336–349, 2018.

[15] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 319–352, 2023.

Biographies

Xu Chen (chenxu18@tsinghua.org.cn) received his B.S. and M.S. degrees from Peking University in 2009 and 2013, respectively. At Tsinghua University, he earned his Ph.D. degree in the Department of Electronic Engineering in 2022. He is now a postdoctoral researcher at Tsinghua University. His research interests include game theory, network management and security.

Wei Feng [SM'13] (fengwei@tsinghua.edu.cn) received the B.S. and Ph.D. degrees from Tsinghua University in 2005 and 2010, respectively. He is currently a Professor with the Department of Electronic Engineering, Tsinghua University. His research interests include maritime communication networks, and coordinated satellite-UAV-terrestrial networks.

Ning Ge [M'97] (gening@tsinghua.edu.cn) received the B.S. and Ph.D. degrees from Tsinghua University in 1993 and 1997, respectively. He is currently a Professor with the Department of Electronics Engineering, Tsinghua University. He has published over 100 papers. His current research interests include communication ASIC design, short range wireless communication, and wireless communications.

Yan Zhang [F'19] (yanzhang@ieee.org) is a full professor with the University of Oslo, Norway. He is a Fellow of IEEE, a Fellow of IET, an Elected Member of Academia Europaea (MAE), the Royal Norwegian Society of Sciences and Letters (DKNVS) and the Norwegian Academy of Technological Sciences (NTVA). His current research interests include next-generation wireless networks leading to 6G and green and secure cyber-physical systems (e.g., smart grid and transport).