ZTEI: Zero-Trust and Edge Intelligence Empowered Continuous Authentication for Satellite Networks

Peiyu Fu[1,2], Jun Wu[1,2,3,4], Xi Lin[1,2,3], and Ao Shen[5]
1.School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China
2.Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai, China
3.Collaborative Innovation Center of Shanghai Industrial Internet, Shanghai, China
4.Faculty of Science and Engineering, Waseda University, Japan
5.Department of Computer Science, Faculty of Engineering, The University of Hong Kong, Hong Kong, China
Email: junwu@aoni.waseda.jp; linxi234@sjtu.edu.cn

GLOBECOM 2022 - 2022 IEEE Global Communications Conference | 978-1-6654-3540-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/GLOBECOM48099.2022.10000958

***Abstract*—The integration of satellite communication technology and terrestrial infrastructure has resulted in an unprecedented increase in network services covering the world. The main effect of the rapid growth of satellite networks is a broader range of data exchange and business interaction between the internal and external systems, making the network boundaries blur or even disappear. As a result, traditional passive security mechanisms based on dividing network boundaries cannot provide sufficient protection. To address this issue, in this paper, we propose a zero-trust and edge intelligence (ZTEI) empowered continuous authentication for satellite networks. We build an improved zero-trust architecture (ZTA) for satellite networks, which expands the traditional zero-trust concept to the multi-dimensional zero-trust that focuses on subject, object, environment, behavior, and physical entity. Then we propose a continuous authentication scheme in the proposed zero-trust architecture, enabling proactive and continuous authentication by periodically monitoring and re-evaluating variable attributes throughout the request lifecycle. Besides, in this scheme, we also design a Neural-Backed Decision Trees (NBDTs) based edge intelligence algorithm to improve the authentication accuracy. Finally, we build a testbed to evaluate the performance of the proposed architecture. Compared with the attribute-based access control (ABAC) under the traditional zero-trust architecture, our proposed architecture can improve the authentication accuracy of dynamic illegal requests by about 27%. In addition, according to standard network performance evaluation criteria, the loss of processing performance caused by our solution is also within an acceptable range.**

***Index Terms*—Zero trust, edge intelligence, continuous authentication, satellite networks**

I. Introduction

In consideration of coverage and cost, most telecom operators and commercial companies have adopted the solution of using satellites to connect edge areas to network [1].The analytics firm Omdia forecasts that cumulative satellite connections will rise fourfold to more than 10 million by 2025 [2]. Due to the lack of basic network security protection measures, network devices and their data are vulnerable to attacks [3]. According to statistics, by 2020, 25% of the attacks received by enterprises are caused by damage to network devices [4]. Attackers often single out vulnerable network devices as the entry point to launch attacks on a broader range of networks and physical entities through Distributed Denial of Service (DDoS) or other attacks [5]. These attacks pose a massive threat to the economy, personal safety, and user privacy, such as the Mirai Botnet's Internet Service Provider DYN attacks [6]. Furthermore, because of the actual needs of satellite networks, we cannot assume that all devices connected to the network or access requests are trustworthy as before [7]. At the same time, the internal security threats brought by connected devices cannot be guaranteed to be eliminated [8]. These facts mean that in the era of satellite networks, the concept of network boundary is gradually blurring or even fading away. Therefore, we cannot only utilize firewalls and intrusion detection systems (IDS) to build network security protection, which means that we must redesign, evaluate, and control the authority and behavior of users, requests, and resources in the satellite networks to ensure the security of the entire network system.

Zero-trust architecture (ZTA) is proposed to be a proper solution to the requirements for security and privacy protection [9]. ZTA transforms network defense from a static division of trust zones and network boundaries to an open architecture that focuses on the in-depth protection of users, assets, and resources. However, the paramount consideration in the design of the existing zero-trust architecture is still the scenario where the subject and object are relatively fixed [10]. The security risk caused by the changes in the state, spatial location, and physical environment of the subject and object are still not fully covered. To this end, we propose an improved ZTA architecture to protect the devices and data of the satellite networks. The main contributions of this paper include:

- We propose an improved zero-trust architecture to improve the coverage and reliability of satellite network security protection. The proposed ZTA extends the security assessment objects into five basic dimensions: subject, object, physical entity, environment, and behavior.
- We propose a continuous authentication scheme in ZTA, which provides periodical, fine-grained session-based access control. In this scheme, we also design an improved neural-supported decision tree based edge intelligence algorithm for improving the accuracy of the continuous

Corresponding authors: Jun Wu and Xi Lin.

authentication.

- We implement and evaluate our proposed architecture using the testbed designed and built by ourselves. The evaluation results demonstrate that our proposed architecture provide the secure authentication and access for the satellite networks under an acceptable performance loss.

The rest of this paper is organized as follows. Section II illustrates the related work about zero-trust architecture, edge intelligence and continuous authentication. In section III, we introduce our design of improved ZTA and continuous authentication scheme. Section IV presents the testing platform and provides evaluation results to show the effect of the proposed architecture. Section V concludes the paper.

II. Related Work

In this section, we review related work in zero-trust architecture, edge intelligence and continuous authentication for satellite networks. We also highlight the impact of the mentioned work on our research.

A. Zero-Trust Architecture

Zero trust, namely "Never Trust and Always Verify," is a security thought and paradigm. According to this paradigm, Zero Trust Architecture (ZTA) is an architecture for designing and implementing network infrastructure construction. It was formally proposed by the National Institute of Standards and Technology (NIST) in 2020 through its Special Publication SP800-207 [11]. ZTA is composed of a data plane and a control plane. The data plane is where network sessions and resource operations occur, while the control plane is responsible for authenticating and authorizing access. The control plane consists of two critical, logical components: policy engine (PE) and policy enforcement point(PEP). PE is responsible for determining the authentication and authorization results. The PEP is located between the resource and the subject and is responsible for executing session management operations.

At present, ZTA is mainly utilized to solve the issues of network boundary disappearance and resource sharing caused by telework or other reasons, such as Google's BcyondCorp5 [10]. Meanwhile, the application of ZTA in next generation networks has received more attention from researchers, and the satellite network is one of them [12].

B. Edge Intelligence for Satellite Networks

In this subsection, we mainly introduce the decision tree algorithm. The decision tree is a tree-like structure consisting of root nodes, internal nodes, and leaf nodes, where each internal node represents a test on an attribute, and each branch represents the test result. Each leaf node represents a class label. The core part of decision tree lies in split finding. How to choose the appropriate feature in the face of massive data and the split position corresponding to the feature is a major difference between different decision tree algorithms. Heuristic class constraint uncertainty and dispersion rate are widely applied feature selection and segmentation criteria. Researchers have proposed different decision tree generation schemes based on these criteria, such as selecting optimal training samples and feature subsets or combining artificial bee colonies and gradient boosted decision trees [13] [14]. In addition, applying artificial intelligence to decision tree algorithms to improve accuracy is also a key research direction.

C. Continuous Authentication in Satellite Networks

Static authentication is the scheme adopted by most satellite network security authentications. It stipulates that the server only verifies the requester just once at the beginning of each session, which is vulnerable to session hijacking attacks [15] [16]. To defend against these attacks, continuous authentication has been introduced. Continuous authentication periodically checks the legitimacy of the requester during the session, protecting against session hijacking or other attacks [17]. There are several researchers have proposed continuous authentication schemes using user biometrics [7] [18] and environmental characteristics for authentication [19]. However, most communicating parties in satellite networks are devices that cannot extract biometrics, and their authentication mechanisms vary from the users' authentication. Thus, strategies like biometrics, memorable patterns, passwords, etc., are insufficient. To solve this issue, we need to expand the coverage of feature extraction to verify devices using features from multiple dimensions to increase the reliability and security of the verification process.

III. The Proposed Multi-Dimensional Zero-Trust Architecture for Satellite Networks

Satellite networks need to achieve collaboration between edge devices and cloud data in a risky, low-latency, and high-concurrency environment [1]. As mentioned in the previous section, current zero-trust architecture is usually established using two basic dimensions: the subject and the object. This dimensional division is not sufficient to satisfy the needs of rapidly evolving satellite network applications. Thus, we extended the concept of existing zero-trust architecture and proposed the architecture shown in Fig. 1. We also proposed a continuous authentication scheme that adopts edge intelligence based on this architecture.

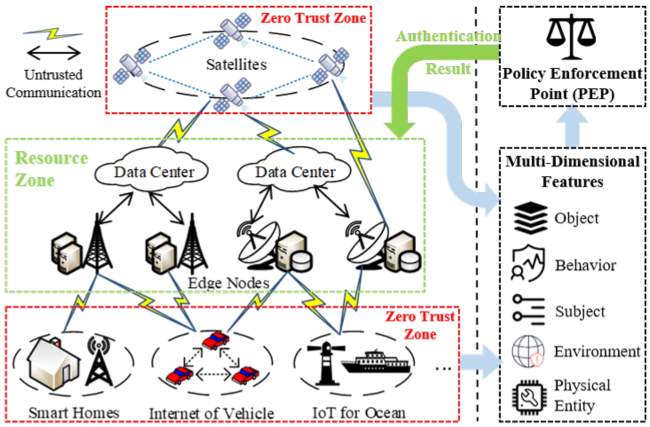

Fig. 1. The multi-dimensional ZTA for satellite network

A. Multi-Dimensional Zero-Trust Architecture

In this subsection, we describe our five-dimensional zero-trust architecture. The five dimensions are: subject, object, environment, behavior and physical entity.

- **Subject of the satellite networks.** The subject is the party in the session that initiates the request. As shown in Fig. 1, in the satellite networks, the subject includes applications, users, and devices located at the edge or cloud. Subjects have different levels of trustability. Generally, subjects with high trustability can access more resources and perform more sensitive operations in the session. The features included in the subject dimension are mainly the subject's identity, preset permissions, and other information extracted to calculate the subject's trustability.
- **Object of the satellite networks.** The object is the resource that is exchanged in a session. As shown in Fig. 1, in the satellite networks, objects are mainly the sensing data from edge sensors, video streaming data from cameras, interfaces provided by edge devices, etc. In common satellite network scenarios, operations on resources usually include uploading, downloading, exchanging, and modifying, and these operations on resources need to be strictly restricted. In general, resources with higher security levels are more limited. The features contained in the object dimension are mainly the information extracted to calculate the security level of objects, such as resource value, demand degree, and threat level.
- **Environment of the satellite networks.** The environment refers to features relevant to session security in the network and real-world situations. As shown in Fig. 1, in the satellite networks, the features of the environment dimension are contained within the features of other dimensions, which are often ignored by existing zero-trust architecture. Usually, the environment in which the two parties are in a conversation has a decisive influence on their security and trust levels. For example, objects located in private domains tend to have a higher level of security, while subjects located in public networks tend to be untrusted. The extraction of environmental features is mainly carried out from two aspects: risk awareness and threat analysis.
- **Behavior dimension in satellite networks.** Behaviors are mainly the records of various operations of subjects and objects on resources and various events that cause dynamic changes in the environment during the session. In the satellite networks, the illegal behavior of some authenticated subjects may cause changes in the subject's trust and even have a significant impact on the entire environment. The feature acquisition channels of the behavior dimension are mainly various log records.
- **Physical entity dimension in the satellite networks.** The physical entity dimension mainly refers to the security-related configuration of edge devices equipped with sensors. As shown in Fig. 1, this type of configuration is frequently fixed information preset before access, which needs to be read in a preset way and extracted as a fundamental condition for security assessment.

B. Continuous Authentication Scheme

The continuous authentication scheme is based on our zero-trust architecture. It takes the 5-dimensional features defined in Section A as inputs for authentication. According to the features of different dimensions, the scheme evaluates the security level of the object and the trust level of the subject respectively. Sessions are authenticated by matching the security level and the trust level. The authentication scheme periodically performs evaluation operations and provides the evaluation results to the policy enforcement point (PDP) to perform zero-trust-based decision operations. When necessary, PDP protects resources by disconnecting the connection.

C. Edge Intelligence for Authentication Mechanism

Since the security authentication mainly decides whether the session is secure, the final result is relatively simple compared with other decision-making processes. Meanwhile, considering the limitations of edge device performance and resources, we choose the decision tree as the decision-making mechanism.

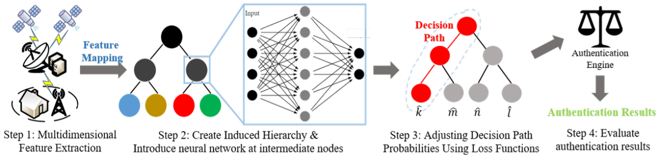
Feature Mapping
Input
Decision Path
$\hat{k}$
$\hat{m}$
$\hat{n}$
$\hat{l}$
Authentication Engine
Authentication Results
Step 1: Multidimensional Feature Extraction
Step 2: Create Induced Hierarchy & Introduce neural network at intermediate nodes
Step 3: Adjusting Decision Path Probabilities Using Loss Functions
Step 4: Evaluate authentication results

Fig. 2. The generation progress of intelligent decision tree

Neural-Backed Decision Trees is a decision tree generation algorithm that combines deep neural network and decision tree proposed by Alvin Wan *et al*. NBDTs replace a network's final linear layer with a decision tree [20]. After introducing NBDT, we build hierarchies based on feature preprocessing and mapping results to reduce overfitting. Due to the uncertainty of intermediate decisions, we choose the path probability calculation scheme proposed in NBDT for inference to improve the tolerance for intermediate decisions. Furthermore, we load our pre-trained model on the nodes of a classical decision tree via NBDT and tune the model using a modified tree supervision loss to guarantee the accuracy of the decision. The specific method is as follows:

We choose soft references provided in the NBDT [20] to construct the final decision probabilities. The final class prediction $\hat{k}$ is defined over these class probabilities, i is a node in a path P_k predicted to be of type k, $C(i)$ contains its child nodes and $p(k)$ is the probability of choosing this path:

$$\hat{k} = argmax_k p(k) = argmax_k \prod_{i \in P_k} p(C_k(i) \mid i). \quad (1)$$

The probability weights assignment may be wrong in the above process due to the lack of standard cross-entropy of inner nodes. To solve this issue, the proposer of NBDT introduces a *tree supervision loss*, a cross-entropy loss over

Algorithm 1 Probability Calculation of Complete Paths in Edge Intelligence

```
Input: $\theta_{ij}, i \in [1,5], j \in R$ for five-dimensional feature; $i \in [1,N]$ for tree nodes; $k \in L(i), i \in [1,K]$ for leaf nodes;
Output: $p(k)$;
$\vec{\gamma}_i = (\theta_{i1}, \theta_{i2}, ..., \theta_{ij})$; for normalized eigenvectors
$\vec{x} = (\gamma_1, \gamma_2, ..., \gamma_5)^T$; for sample features
for all $k \in L(i), i \in [K+1, N]$ do
    $n_i = \sum_{k \in L(i)} w_k / |L(i)|$;
end for

for all $k \in L(i)$ do
    find all paths: $P_k$
    for all $i \in P_k$ do
        calculate $p(C_k(i) \mid i)$, $C_k(i) \in P_k \cap C(i)$
    end for
    $p(k) = \prod_{i \in P_k} p(C_k(i) \mid i)$
end for
return $p(k)$
```

the class distribution of path probabilities $\mathcal{D}_{nbdt} = \{p(k)\}_{k=1}^{K}$, with time-varying weights. In this paper, we modify the *tree supervision loss* according to the actual scene. The calculation method is as follows: the function $H(x, y)$ is used to calculate the binary cross-entropy. ω_t and β_t are the time-varying weights.

$$H_t(\mathcal{D}) = -\frac{1}{K}\sum_{i=1}^{K} \mathcal{D} \cdot log(\mathcal{D}) + (1 - \mathcal{D}) \cdot log(1 - \mathcal{D}). \quad (2)$$

$$\mathcal{L} = \omega_t H(\mathcal{D}_{nbdt}) + \beta_t H(\mathcal{D}_{nbdt}). \quad (3)$$

Taking the final decision probability as the raw decisions of the authentication, we obtain the final edge intelligent decision tree model for security assessment and decision. For each access request Q, $t \in T$ is any timestamp during this request (timestamps are calculated as the minimum interval during continuous authentications). The above decision tree model could obtain a result with the value of $v_t \in V$, and its trustable probability is p_t. Then the evaluation value $\mathcal{A}_t$ of the request at the t is:

$$\mathcal{A}_t = \begin{cases} v_t \times p_t - v_{t-1}(p_{t-1} - p_t), & p_t < p_{t-1}, \\ v_t \times p_t, & p_t \geq p_{t-1} \ or \ \ v_t < v_{t-1}. \end{cases} \quad (4)$$

By selecting different feature parameters and mapping the features differently, we can obtain the security level evaluation decision for the server and the trust level evaluation decision for the requester. After obtaining the evaluation value of both parties through the corresponding decision (T_t, S_t), we can get the final authentication result. The request is allowed if and only if the security level evaluation decision and the trust level evaluation decision satisfy $T_t >= S_t, t \in [\tau, t]$. In any other case, the access request shall be denied immediately, or the established connection shall be disconnected.

IV. Evaluation

To verify the impact of our proposed zero-trust architecture and continuous authentication scheme on the efficiency of satellite network systems, we built an testbed. Under the premise of guaranteeing continuous certification functionality, our evaluation mainly focuses on three parts: 1) security protection performance evaluation, 2) startup evaluation, and 3) runtime evaluation. The security protection performance evaluation is used to verify the protective effect of the proposed scheme against common attacks. The startup evaluation mainly reflects the performance changes of the system after the solution is integrated when it faces the increase or decrease of devices or when it goes offline. The runtime evaluation shows the impact of the solution's integration on the system's processing power. To demonstrate the performance of our proposed architecture and scheme more intuitively, we the following sets of comparative experiments: 1) **our proposed architecture and scheme**, which is referred to as EID, 2) **traditional ZTA and its attribute-based access control scheme**, which is referred as ABAC.

A. Test Environment

According to the evaluation requirements, we built a test environment. This test environment including protected satellite network modules (simulated using a Raspberry Pi), terrestrial IoT device modules, authentication modules, and untrusted user modules. In this test environment, information from the different modules was gathered into the authentication module for continuous trust assessment. We use PCs and mobile phones to simulate session requests and evaluate the effect of continuous authentication. The evaluation was performed on a virtual machine equipped with 2 GB of RAM, CPU Intel Core i5 ®8600K @ 3.60GHz, and running Ubuntu Linux OS.

B. Security Protection Performance Evaluation

We evaluate the performance of the proposed scheme on security protection, and we choose attribute-based access control as the control. We simulate requests from different origins by sending requests from different terminals to the testbed, where the ratio of legitimate/illegal requests is 3:7. We define the above request as a static request. After completing the test, we resend the same request. 50% of the authenticated requests are selected to perform illegal operations during the session in this request process. We define such requests as dynamic requests. The identification results of different schemes for requests are shown in Table I.

TABLE I
Authentication accuracy of requests for different schemes

Method	Static Request	Dynamic Request
ABAC	92.04%	68.49%
EID	94.61%	86.97%

The results in Table I show that our proposed scheme has good accuracy for identifying dynamic illegal requests and can effectively reduce the risk of connected devices being subjected to hijacking attacks.

C. Comparison on Startup Time

We evaluate the impact on system startup progress with other scheme. We define the startup response time as when the system starts, the time from the pre-trained of the access control policy method to when the access control service can be provided externally. In practical applications, there are usually two startup situations. 1) Cold start: The system does not load any attributes, and the set attributes need to be pre-loaded and pre-trained for edge intelligent decision before starting. Cold start corresponds to the system startup situation when a large number of devices are initially deployed in practical application scenarios. 2) Standard run: The loading of attributes and the pre-training of edge decision trees have been completed. The standard operation corresponds to the reconnection after some devices are offline in practical application scenarios.

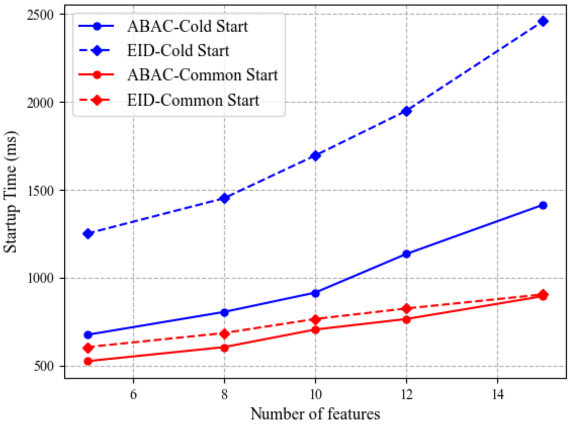

Fig. 3. Startup time under different number of features in different situation

Fig. 3 shows the startup time of different architectures and schemes under different situations when selecting a different number of features. We perform 1000 replicates, and it should be noted that the data obtained during the experiment can vary within a fairly significant range due to the relatively small performance. To ensure that the data matches the actual situation as much as possible, we have processed some abnormal data and deleted the data that cannot be reproduced. It can be found from the figure that under the cold-start condition, the startup response time increases significantly with the increase of the dimensions involved in the evaluation, and the time consumption of the strategy based on edge intelligence is substantially higher than that of the common methods. But the cold start only occurs when the satellite system is running for the first time or when a large number of new devices are connected simultaneously, which is almost negligible compared to the uptime of the satellite networks. In most cases, we should consider the restart time of satellite networks in standard operating scenarios. It can be found from Fig. 3 that at this time, the time consumption decreases significantly with the growth rate of the number of attributes, and the time-consuming gap between different strategies is gradually reduced or even almost the same. The above data show that our proposed architecture and scheme will not significantly impact the system during startup under the normal situation.

D. Comparison on Runtime of Continuous Authentication

We evaluate the impact of our proposed architecture and scheme on processing performance after startup. We divide the test evaluation into two parts: 1) Under low load conditions, evaluate the impact of different attribute numbers on the runtime of continuous authentication; 2) Select an appropriate number of attributes to evaluate the runtime of different schemes under high load conditions. To eliminate the influence of the difference in the number of internal and external requests from the satellite network application on the results as much as possible, we count the distribution of requests when the testbed is running regularly. Fig. 4 and Fig. 5 show the results after running 1000 experiments.

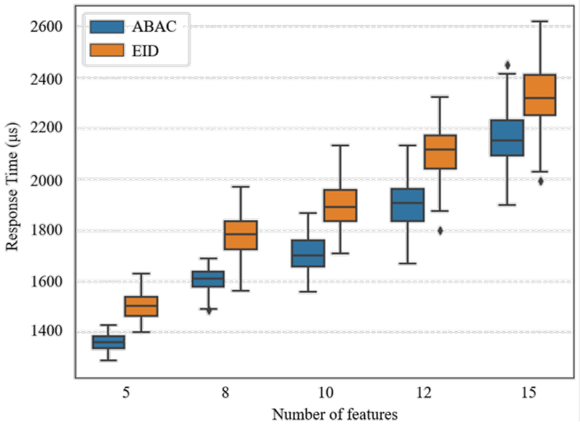

Fig. 4. Runtime under different number of features

Fig. 4 shows the relationship between decision time and the number of attributes involved in the decision under low load conditions. As the number of attributes involved in decision increases, the time consumption of a single decision increases gradually, and the variance increases as a whole. At the same time, the time consumed by the strategy based on edge intelligence is also slightly higher than that of the general scheme. However, considering the proportion of decision time in a single request time, the increase in decision time is still within an acceptable range. Therefore, we can draw the following conclusions: the performance of our proposed continuous authentication scheme under low load is almost the same as that of the current common schemes, and will not have a large impact on the performance of the satellite network system.

Based on the experimental results in Fig. 4, we set the number of attributes to be 10 under high load. By gradually increasing the number of concurrent requests, we obtain the relationship between the decision time for high load conditions and the number of concurrent requests, as shown in Fig. 5. The data in the figure shows that with the increase of the number of concurrent requests, the decision time of the common strategy

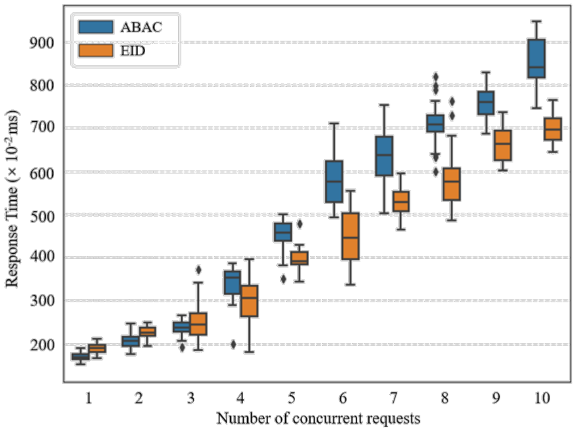

Fig. 5. Runtime under different number of concurrent requests

grows significantly faster than that of the strategy based on edge intelligence, which causes the decision time of the former to eventually exceed the latter. At the same time, when the number of concurrency is high, the runtime of common strategies fluctuates within a large range, while the strategies based on edge intelligence are relatively stable. Therefore, we can draw the following conclusions: the processing capability of our proposed continuous authentication scheme is relatively stable under high load conditions, and has little impact on the overall processing performance of the system.

V. Conclusion And Future Work

This paper proposed a multi-dimensional zero-trust architecture and continuous authentication scheme for satellite networks based on the proposed ZTA and edge intelligence. Driven by satellite network-associated security challenges, we proposed a multi-dimensional zero-trust architecture. Then we designed a continuous authentication scheme in zero-trust architecture based on the proposed architecture. This scheme takes advantage of the edge intelligence, specifically a Neural-Backed Decision Tree, to evaluate multi-dimensional attributes of requests and implement corresponding security operations according to the decision results. We evaluated the scheme on our testbed. The evaluation results show that this scheme can meet the limitations of satellite network devices in terms of performance, storage, and computing and can effectively solve the security access control issue in satellite networks. In future work, we aim to improve the efficiency of continuous authentication by enhancing the edge intelligence algorithm. We also plan to introduce technologies such as blockchain to ensure the security of policies and decisions in transit.

ACKNOWLEDGMENT

This work is supported in part by the National Natural Science Foundation of China under Grant No. U21B2019 and 61972255, and in part by the Science and Technology on Communication Security Laboratory Foundation (61421030208012106).

References

[1] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, “A survey on technologies, standards and open challenges in satellite iot,” *IEEE Communications Surveys Tutorials*, vol. 23, no. 3, pp. 1693–1720, 2021.

[2] S. Lucero, “Satellite iot market repot 2020,” London, U.K., Mar., Tech. Rep., 2020.

[3] K.-Y. Lam, S. Mitra, F. Gondesen, and X. Yi, “Ant-centric iot security reference architecture—security-by-design for satellite-enabled smart cities,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5895–5908, 2022.

[4] T. Dimitrakos, T. Dilshener, A. Kravtsov, A. La Marra, F. Martinelli, A. Rizos, A. Rosetti, and A. Saracino, “Trust aware continuous authorization for zero trust in consumer internet of things,” in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1801–1812.

[5] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “Ddos in the iot: Mirai and other botnets,” *Computer*, vol. 50, no. 7, p. 80–84, jan 2017. [Online]. Available: https://doi.org/10.1109/MC.2017.201

[6] J. Lee, J. Kim, and J. Seo, “Cyber attack scenarios on smart city and their ripple effects,” in *2019 International Conference on Platform Technology and Service (PlatCon)*, 2019, pp. 1–5.

[7] A.-E. M. Taha and A. Elabd, “Iot for certified sustainability in smart buildings,” *IEEE Network*, vol. 35, no. 4, pp. 241–247, 2021.

[8] X. Lin, J. Wu, J. Li, X. Zheng, and G. Li, “Friend-as-learner: Socially-driven trustworthy and efficient wireless federated edge learning,” *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[9] A. Wylde, “Zero trust: Never trust, always verify,” in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, pp. 1–4.

[10] A. P. Patil, G. Karkal, J. Wadhwa, M. Sawood, and K. Dhanush Reddy, “Design and implementation of a consensus algorithm to build zero trust model,” in *2020 IEEE 17th India Council International Conference (INDICON)*, 2020, pp. 1–5.

[11] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture (2nd draft),” National Institute of Standards and Technology, Tech. Rep., 2020.

[12] S. Li, “Zero trust based internet of things,” *EAI Endorsed Transactions on Internet of Things*, vol. 5, no. 20, 2020.

[13] N. E. I. Karabadji, I. Khelf, H. Seridi, S. Aridhi, D. Rémond, and W. Dhifli, “A data sampling and attribute selection strategy for improving decision tree construction,” *Expert Systems with Applications*, vol. 129, pp. 84–96, 2019.

[14] H. Rao, X. Shi, A. K. Rodrigue, J. Feng, Y. Xia, M. Elhoseny, X. Yuan, and L. Gu, “Feature selection based on artificial bee colony and gradient boosting decision tree,” *Applied Soft Computing*, vol. 74, pp. 634–642, 2019.

[15] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K.-K. R. Choo, and G. Min, “A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things,” *IEEE Transactions on Computers*, pp. 1–1, 2022.

[16] X. Lin, J. Wu, J. Li, W. Yang, and M. Guizani, “Stochastic digital-twin service demand with edge response: An incentive-based congestion control approach,” *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[17] H. Kong, L. Lu, J. Yu, Y. Chen, and F. Tang, “Continuous authentication through finger gesture interaction for smart homes using wifi,” *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3148–3162, 2021.

[18] Y. Liang, S. Samtani, B. Guo, and Z. Yu, “Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.

[19] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trust management in decentralized iot access control system,” in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[20] A. Wan, L. Dunlap, D. Ho, J. Yin, S. Lee, H. Jin, S. Petryk, S. A. Bargal, and J. E. Gonzalez, “NBDT: neural-backed decision trees,” *CoRR*, vol. abs/2004.00221, 2020. [Online]. Available: https://arxiv.org/abs/2004.00221