Secure Application of MIoT

Subjects: Computer Science, Cybernetics

Contributor: Jiming Yin, Jie Cui

With the increasing demand for higher-quality services, online English education platforms have gained significant attention. However, practical application of the Mobile Internet of Things (MIoT) still faces various challenges, including communication security, availability, scalability, etc. These challenges directly impact the utilization of online English education platforms. The dynamic and evolving nature of the topology characteristics in Mobile Internet of Things networks adds complexity to addressing these issues.

Keywords: MIoT ; software-defined MIoT ; signature ; authentication ; online English education

1. Introduction

The Internet of Things (IoT) has drawn attention from both industry and academic fields for years due to its advantages, such as efficiency and providing more secure communication environments. Among the various applications of IoT, online education has emerged as a significant application of Mobile IoT (MIoT). IoT provides the necessary technological support and infrastructure for online education to be conducted on mobile devices and over the Internet. English, being a globally universal language, is widely learned and considered a core subject in schools across most countries. Consequently, the application of MIoT in online English education has rapidly become an important method and primary tool for individual learning and communication. This is a novel education model that puts students at the center and relies on software platforms to deliver personalized learning experiences [1][2]. Compared to traditional offline classroom education, online English education offers advantages such as higher efficiency [3][4] and freedom from geographical constraints [5]. Here, online learning devices (OLDs) have the capability to communicate with other devices and infrastructure, such as roadside units in certain models, enabling access to the MIoT [6]. Thus, OLDs are allowed to report information and emergencies, which will be used to improve the quality of services [7][8]. However, if OLDs are allowed to broadcast messages without any verification or limitation, the communication mechanism will become vulnerable and easy to compromise [9][10][11]. For example, if messages sent in MIoT are not signed with an online learning device's unique identities, then a malicious user can broadcast fraud messages or sign them with fabricated identities to bypass a weak system. To solve problems in secure communication, some studies have been dedicated to designing privacy-preserving authentication schemes [12][13][14]. However, due to the feature of changing topology, it is hard to balance efficiency and security in conventional MIoT. Then, a brand-new technology came into researchers' sights.

Software-defined network (SDN) is an innovative technology that embodies a network structure distinct from traditional networks [15][16]. In SDN, controlling and forwarding are separated and work in different layers [17][18]. The control plane represents the centralized point as the brain of the whole architecture [19]. The data plane communicates with the control plane via southbound interfaces. It is mainly responsible for querying controllers for forwarding tables and forward packets. Using the programmability and scalability, the combination of VANETs and SDN offers a new approach to solve inherent problems in VANETs.

Software-defined MIoT has been proposed for years and there have been many research efforts demonstrating the advantages of this new combination [20][21]. Meanwhile, some schemes are proposed to cope with problems in quality of services (QoS) [22], heterogeneous network accessing [23], factory managing [24][25] and so many others in different fields by combining with SDN [26]. Inspired by [27], the design a scheme that uses multicast technology to solve the driving direction and secure communication problems in software-defined MIoT.

In traditional MIoT, OLDs mainly rely on broadcasting each other to receive network condition information, which lacks timeliness and overall planning [28][29][30]. By introducing multicast, the controller is allowed to manage OLDs and balance network throughputs more efficiently. In addition, some technology used not to be suitable for MIoT, like Steiner Tree, which is computation intense and scale sensitive [27]. But with SDN introduced, those algorithms can provide new methods for the development of MIoT [31][32].

2. Leveraging IoT and Cloud for Enhanced Online Education

Online education has a significant impact on the learning process by leveraging the IoT, cloud computing and big data. The key to integrating online educational resources lies in the storage of massive teaching data. Wei et al. [33] applied cloud storage technologies and methods to the construction of integrated online educational resources, which effectively saves educational resources for schools, enhances the utilization of online educational resources and thereby improves the teaching quality of subjects. Hui Tao [34] proposed an online English teaching system approach based on IoT technology. The author studied the English SPOC (Small Private Online Course) teaching mode, constructed a multimedia teaching system based on IoT technology, improved the teaching system and enhanced and learned the teaching mode, resulting in an improvement in the quality of English teaching.

Chen et al. [35] developed an IoT-oriented online English education platform with the aim of providing a conducive learning environment and enhancing students' overall English proficiency. To improve the ability to find optimal solutions, they incorporated a reverse learning (RL) mechanism into the grey wolf optimization (GWO) algorithm, resulting in the development of the RLGWO algorithm. They further constructed the RLGWO-BP model, which was utilized to assess the impact of the IoT-oriented online education platform on English language instruction. Gao et al. [36] utilized preliminary results obtained through the use of IoT to establish an interactive educational paradigm. They deployed numerous sensors with the aim of improving learners' English language correction by comparing learners' wording and speech with the software's standard wording and speech.

In the security in MIoT and the software-defined MIoT research field, a threshold anonymous authentication protocol using group signature technology was proposed by Shao et al. [9]. In this scheme, the decentralized group model is integrated. It achieved threshold authentication, anonymity, unforgeability, tracability and revocation of MIoT communication. However, the huge computation cost of bilinear pairing may create obstacles to implementation. Azees et al. [37] proposed a scheme that enabled roadside units to authenticate vehicles anonymously before providing certain messages to them. It also allowed vehicles to communicate with roadside units anonymously. The scheme reduced costs of certificate and signature verification and achieved privacy preserving and traceability in vehicular ad hoc networks. However, there were no timestamps attached to messages, which could be used by malicious parities to start replay attacks.

To solve the problems of insecurity of master keys, invalidity of PIDs in [12], and to cope with inherent problems in MIoT, Li et al. [38] proposed a certificate-less protocol and demonstrated the security of it. Xiang et al. [39] proposed a novel CLS (certificate-less signcryption) scheme to address critical issues such as data integrity and identity authentication in the IoT environment. The scheme eliminates the cumbersome certificate management in certificate-based signature systems and the key escrow problem in identity-based cryptography. Furthermore, it is designed to securely resist various attacks, such as public key-replacement attacks or malicious but passive key-generation center attacks. Garg et al. [31] proposed secure communication models by introducing SDN architecture. They enabled both mutual authentication among communicating entities and intrusion-detecting systems to detect potential attacks from the underling networks.

Hong et al. [40] proposed a time-limited secure attribute-based online/offline signature scheme (TS-ABOS-CMS) with a constant message length. The scheme achieves high efficiency by introducing online/offline signature methods while maintaining communication overhead at a constant level. Additionally, a key update mechanism is adopted to provide time-limited security protection for IoT terminals. Khashan et al. [41] proposed a blockchain-based hybrid centralized IoT system authentication architecture. Edge servers are deployed to provide centralized authentication for associated IoT devices. Subsequently, a blockchain network is established for the centralized edge servers to ensure decentralized authentication and verification of IoT devices belonging to different and heterogeneous IoT systems. Wang et al. [42] adopted the low-energy distributed ledger technology IOTA to design a lightweight and scalable mechanism for managing the identity of IoT devices and access control of large-scale IoT data. This mechanism ensures the reliability of the source of IoT data and the security of data sharing.

In the multicast in the SDN research field, Zhou et al. [27] proposed the cost-efficient Degree-dependent Branch-node Weighted Steiner Tree (DBWST) problem in the SDN architecture. It solved the scalability problem of multicast by introducing Steiner Tree to span nodes. The scheme reduced the total cost and the number of branch nodes when generating the multicast tree T. Do et al. [26] proposed an architecture that allowed both multicast and broadcast services in the SDN-based mobile packet core. It had the advantages of programmability and flexibility of SDN and reduced the signaling cost compared with traditional network paradigms. However, the system may suffer certain security problems in terms of communication.

Lai et al. [43] proposed an integrated network architecture for secure group communication in SDN-based 5G vehicular ad hoc networks. The scheme was a group-oriented vehicular environment, in which vehicles are divided into groups based on their geographic positions. This also inspired researchers to manage vehicles by dividing them in a transaction-oriented way. Kim et al. [24] proposed a multicast scheme with Group Shared Tree (GST) switching in large-scale IIoT networks. To overcome inherent problems, such as transmitting multicast packets under congestions and configuring optimal paths dynamically, it adopted SDN-based architecture. They proved that the new architecture outperformed other models.

References

1. Gómez, J.; Huete, J.F.; Hoyos, O.; Perezc, L.; Grigorid, D. Interaction system based on Internet of Things as support for education. Procedia Comput. Sci. 2013, 21, 132–139.
2. Gul, S.; Asif, M.; Ahmad, S.; Yasir, M.; Majid, M.; Malik, M.S.A. A survey on role of Internet of Things in education. Int. J. Comput. Sci. Netw. Secur. 2017, 17, 159–165.
3. Konan, M.; Wang, W. A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. Sensors 2019, 19, 1608–1621.
4. Vasile, R.; Olivares, S.; Paris, M.G.A.; Maniscalco, S. Continuous-variable quantum key distribution in non-Markovian channels. Phys. Rev. A 2011, 83, 042321.
5. Pei, X.L.; Wang, X.; Wang, Y.F.; Li, M.K. Internet of Things based education: Definition, benefits and challenges. Appl. Mech. Mater. 2013, 411, 2947–2951.
6. Li, J.L.; Choo, K.K.R.; Zhang, W.; Kumari, S.; Joel, J.P.C.R.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. Veh. Commun. 2018, 13, 104–113.
7. Liu, Y.; Wang, Y.; Chang, G. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2740–2749.
8. Phoenix, S.; Khan, F.; Teklu, B. Preferences in quantum games. Phys. Lett. A 2020, 384, 126299.
9. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. IEEE Trans. Veh. Technol. 2015, 65, 1711–1720.
10. Trapani, J.; Teklu, B.; Olivares, S.; Paris, M.G.A. Quantum phase communication channels in the presence of static and dynamical phase diffusion. Phys. Rev. A 2015, 92, 012317.
11. Wang, M.; Liu, D.; Zhu, L.; Xu, Y.; Wang, F. LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing 2016, 98, 685–708.
12. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. J. Abbr. 2015, 10, 2681–2691.
13. Huang, J.; Qian, Y.; Hu, R.Q. Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software Defined Vehicular Networks. IEEE Trans. Veh. Technol. 2020, 69, 8542–8554.
14. Cui, J.; Zhang, X.; Zhong, H.; Zhang, J.; Liu, L. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. IEEE Trans. Inf. Forensics Secur. 2019, 15, 1654–1667.
15. Li, H.; Dong, M.; Ota, K. Control plane optimization in software-defined vehicular ad hoc networks. IEEE Trans. Veh. Technol. 2016, 65, 7895–7904.
16. Rosati, M.; Mari, A.; Giovannetti, V. Coherent-state discrimination via nonheralded probabilistic amplification. Phys. Rev. A 2016, 93, 062315.
17. Duan, P.; Peng, C.; Zhu, Q.; Shi, J.; Cai, H. Design and analysis of software defined Vehicular Cyber Physical Systems. In Proceedings of the 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, 16–19 December 2014; pp. 412–417.
18. Teklu, B.; Bina, M.; Paris, M.G.A. Noisy propagation of Gaussian states in optical media with finite bandwidth. Sci. Rep. 2022, 12, 11646.
19. de Oca, E.M.; Mallouli, W. Security Aspects of SDMN. In Software Defined Mobile Networks (SDMN) beyond LTE Network Architecture; IEEE: Piscataway, NJ, USA, 2015; pp. 331–357.
20. Nkenyereye, L.; Nkenyereye, L.; Islam, S.M.R.; Choi, Y.H.; Bilal, M.; Jang, J.W. Software-defined network-based vehicular networks: A position paper on their modeling and implementation. Sensors 2019, 19, 3788.

21. Zhu, M.; Cao, J.; Pang, D.; He, Z.; Xu, M. SDN-based routing for efficient message propagation in VANET. In Wireless Algorithms, Systems and Applications: 10th International Conference, Qufu, China, 10–12 August 2015; Springer International Publishing: Berlin/Heidelberg, Germany, 2015; pp. 788–797.
22. Karakus, M.; Durresi, A. Quality of service (QoS) in software defined networking (SDN): A survey. J. Netw. Comput. Appl. 2017, 10, 2681–2691.
23. Lai, C.; Lu, R.; Zheng, D. Achieving secure and seamless IP Communications for group-oriented software defined vehicular networks. Wirel. Algorithms Syst. 2017, 10, 356–368.
24. Kim, H.S.; Yun, S.; Kim, H.; Shin, H.; Kim, W.T. An efficient SDN multicast architecture for dynamic industrial IoT environments. Mob. Inf. Syst. 2018, 2018, 8482467.
25. Teklu, B. Continuous-variable entanglement dynamics in Lorentzian environment. Phys. Lett. A 2022, 432, 128022.
26. Do, T.X.; Nguyen, V.G.; Kim, Y. SDN-based mobile packet core for multicast and broadcast services. Wirel. Netw. 2018, 24, 1715–1728.
27. Zhou, S.; Wang, H.; Yi, S.; Zhu, F. Cost-efficient and scalable multicast tree in software defined networking. In Proceedings of the Algorithms and Architectures for Parallel Processing: 15th International Conference, ICA3PP 2015, Zhangjiajie, China, 18–20 November 2015; pp. 592–605.
28. Lecompte, D.; Gabin, F. Evolved multimedia broadcast/multicast service (eMBMS) in LTE-advanced: Overview and Rel-11 enhancements. IEEE Commun. Mag. 2012, 50, 68–74.
29. Chen, J.; Yan, F.; Li, D.; Chen, S.; Qiu, X. Recovery and Reconstruction of Multicast Tree in Software-Defined Network: High Speed and Low Cost. IEEE Access 2020, 8, 27188–27201.
30. Teklu, B.; Trapani, J.; Olivares, S.; Paris, M.G.A. Noisy quantum phase communication channels. Phys. Scr. 2015, 90, 074027.
31. Garg, S.; Kaur, K.; Kaddoum, G.; Ahmed, S.H.; Jayakody, D.N.K. SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective. IEEE Trans. Veh. Technol. 2019, 68, 8421–8434.
32. Adnane, H.; Teklu, B.; Paris, M.G.A. Quantum phase communication channels assisted by non-deterministic noiseless amplifiers. JOSA B 2019, 36, 2938–2945.
33. Li, W.; Guo, Y. A Secure Private Cloud Storage Platform for English Education Resources Based on IoT Technology. Comput. Math. Methods Med. 2022, 2022, 8453470.
34. Tao, H. Online English Teaching System Based on Internet of Things Technology. J. Sens. 2022, 2022, 7748067.
35. Chen, D. Application of IoT-Oriented Online Education Platform in English Teaching. Math. Probl. Eng. 2022, 2022, 9606706.
36. Gao, W. Designing an interactive teaching model of English language using Internet of Things. Soft Comput. 2022, 26, 10903–10913.
37. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans. Intell. Transp. 2017, 18, 2467–2476.
38. Li, J.; Ji, Y.; Choo, K.K.R.; Hogrefe, D. CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the Internet of Vehicles. IEEE Internet Things J. 2019, 6, 10332–10343.
39. Xiang, D.; Li, X.; Gao, J.; Zhang, X. A secure and efficient certificateless signature scheme for Internet of Things. Ad Hoc Netw. 2022, 124, 102702.
40. Hong, H.; Sun, Z. TS-ABOS-CMS: Time-bounded secure attribute-based online/offline signature with constant message size for IoT systems. J. Syst. Archit. 2022, 123, 102388.
41. Khashan, O.A.; Khafajah, N.M. Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. J. King Saud Univ.-Comput. Inf. Sci. 2023, 35, 726–739.
42. Wang, S.; Li, H.; Chen, J.; Wang, J.; Deng, Y. DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. J. Inf. Secur. Appl. 2022, 66, 103134.
43. Lai, C.; Zhou, H.; Cheng, N.; Shen, X.S. Secure group communications in vehicular networks: A software-defined network-enabled architecture and solution. IEEE Veh. Technol. Mag. 2017, 12, 40–49.