ID-Based SDN for the Internet of Things

Xiaoliang Wang, Ke Xu, Wenlong Chen, Qi Li, Meng Shen, and Bo Wu

Abstract

The rapid development of the Internet of Things (IoT) has made impressive achievements, raising a heated discussion about IoT big data, in which data security and privacy issues are key concerns. Due to the ubiquity of IoT, IoT big data has not only brought convenience to people's daily lives, but also increased the potential attack surfaces for cybercriminals. At the same time, considering the characteristics of resource constraints and heterogeneity, with traditional network security solutions it can be difficult to achieve ideal results in the IoT environment, which further exacerbates the challenges faced by IoT big data security. In this case, the advantages introduced by software defined networking (SDN) have the potential to meet the challenges of IoT security risks. To this aim, we propose an ID-based SDN secure network architecture called IBSDN. Different from the traditional SDN solution, IBSDN is committed to providing IoT with endogenous trusted services on the network side by embedding unforgeable terminal identities in the data stream. This network-level trusted service can prevent IoT terminals from consuming restricted resources for the sake of security, providing greater scalability and manageability for network security monitoring.

Introduction

With the rapid development of network technologies, mobile computing, and artificial intelligence, people's demand for intelligent life is increasing. Under this trend, the Internet of Things (IoT) has also achieved remarkable results in recent years. The IoT industry is believed to bring a wealth of business opportunities and significantly accelerate the development of IoT-based services. According to McKinsey's business report on the global IoT industry, the annual commercial impact of IoT will be in the range of $2.7 to $6.2 trillion by 2025. These business expectations imply that the IoT industry and the big data services it brings will usher in huge and rapid growth in the coming years.

IoT is known to be one of the major sources of big data, as it is based on connecting a huge number of smart devices to the Internet to report their frequently captured status of their environments. These ubiquitous connections and resulting big data can bring significant improvements in each area of human life, such as industry, agriculture, transportation, and smart cities. Numerous smart IoT terminals will build a bridge between the virtual and real worlds through perception and feedback, thus making our living environment much smarter. To achieve this goal, IoT devices can interoperate or provide unified data services with back-end system support, for example, when processing the big data generated by sensing activities [13].

On the other hand, the ubiquity of the IoT systems and the emerging new application scenarios can introduce new potential attack surfaces for cybercriminals. For example, under the guidance of smart manufacturing, a large number of IoT devices and technologies are applied in industrial control systems. Attacks against these industrial control systems can lead to serious production failures, resulting in quality degradation and even the risk of casualties. In addition, since IoT applications are closer to the environment in which we live than ever before, data integrity and privacy protection will face unprecedented challenges. It is not hard to imagine the serious consequences of leakage of sensitive information caused by home monitoring or medical systems. At the same time, due to the heterogeneity and complexity of IoT systems, the complexity of security mechanism management in different industries and scenarios will be amplified in a unified way. Finally, we also need to recognize that resource-constrained IoT devices are more vulnerable to malicious users than traditional network terminals, which means that the defense capabilities of single points in IoT networks may be the weakest link in the entire system. Even a single compromised node may cause harm to other nodes and affect the performance of system service. For the security dilemma faced by IoT systems, we need systematic and comprehensive network management and security monitoring capabilities.

Through the above analysis, we realize that the resource-constrained and heterogeneous nature of IoT systems makes the classic security solution difficult to apply to the IoT environment, therefore requiring a network-based trusted mechanism to achieve scalability and highly efficient security [14]. At present, there are research efforts focusing on the technology integration of software defined networking (SDN) and IoT [3]. Because of the technical characteristics of network virtualization and centralized control, SDN also has a strong competitive advantage in the face of heterogeneous and distributed security threats. These

Xiaoliang Wang and Wenlong Chen are with Capital Normal University; Ke Xu and Qi Li are with Tsinghua University and the Beijing National Research Center for Information Science and Technology; Meng Shen is with Beijing Institute of Technology; Bo Wu is with Huawei Technologies. Ke Xu and Meng Chen are also with Peng Cheng Laboratory.

Digital Object Identifier:
10.1109/MNET.011.1900380

0890-8044/20/$25.00 © 2020 IEEE

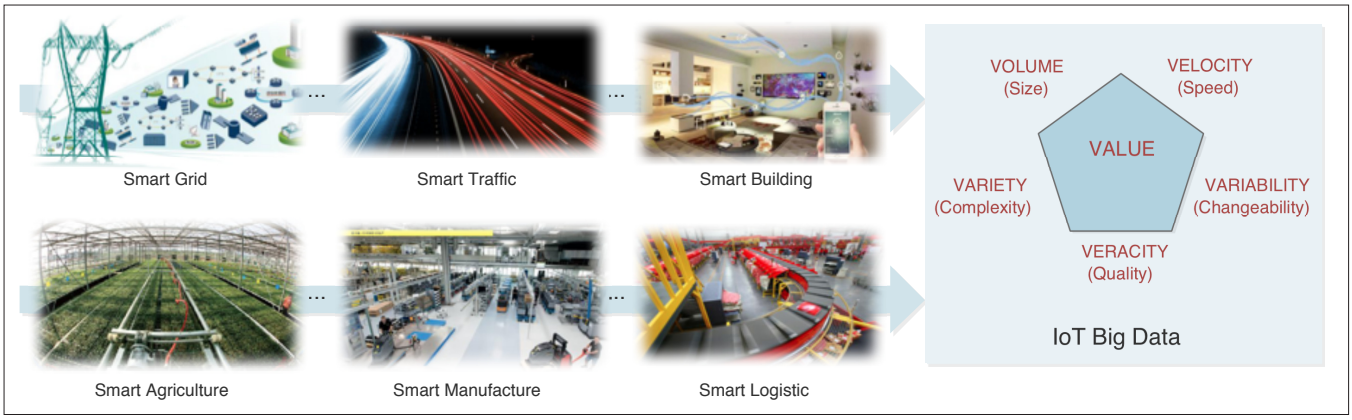

FIGURE 1. IoT big data.

give SDN the potential to meet the challenges of IoT security risks.

In this article, we propose an ID-based SDN security architecture called IBSDN. In this architecture, we first make the device's IP address unforgeable through address authenticity guarantee before embedding the device identity information into an IPv6 address. On this basis, the classic SDN network can implement centralized management of IoT network behaviors based on terminal identity through IP address and flow table without excessive modification. At the same time, the granularity of traffic monitoring and management can be refined to the packet level. This will bring authentication and basic trust services with no device side overhead for IoT communications, and several other advantages in terms of flexibility and manageability.

IoT Big Data and Security Threats

It is worth noticing that IoT big data is based on IoT ubiquitousness and the frequent acquisition of the state of the surrounding environment by sensing devices. The value of big data lies in identifying valuable associations and information patterns from a vast amount of data. Big data can help to understand the data from higher levels of insights and guide future decisions. Some researchers have discussed and described the overall characteristics of big data [10–12], and we use the following 6V features (as shown in Fig. 1) to analyze IoT big data:

Volume: IoT devices cover many aspects of people's daily lives, from manufacturing to personal health, from transportation to agriculture. IoT systems involve a large number of terminal devices that are used to monitor environmental status. The frequent data collection combined with numerous terminal devices have resulted in a huge amount of data for IoT.

Variety: From an overall perspective, IoT services cover many areas of people's lives. The service form and the contents are highly heterogeneous, leading to a large variety of categories of IoT data. Even if only focusing on a specific application scenario, the difference of manufacturers, equipment models, and system design mean that the specific form of the data collected by the terminal devices will vary widely. For example, for an indoor temperature control system, some manufacturers may only use terminal devices to collect the current room temperature and receive the temperature control instructions issued by the cloud service, while others may use the terminal system to collect GPS information and obtain local weather conditions for comprehensive assessment of temperature control. These functional design differences also increase the category differences in IoT data.

Velocity: Considering that a large number of IoT applications monitor the state of the surrounding environment or control the production process in real time, the data generation rate and the streaming rate of the IoT big data are high. The huge number of terminals coupled with the high data generation rate is sufficient to the needs of real-time big data analytics services, which is one reason why IoT big data has received a lot of attention.

Varibility: Since IoT devices are usually used to perceive the surrounding environment, the resulting specific data, data categories, and data generation rates are largely influenced by the surrounding environment and are constantly changing. For security monitoring systems, the collection rate of information is significantly higher than the stable operating state when unknown intrusions are detected. For traffic monitoring systems, because the urban traffic conditions vary at different time periods, the IoT data collected by a traffic monitoring system also has the corresponding differences.

Veracity: Authenticity is the foundation of the value of big data, and in IoT systems, the vast majority of data is collected directly from terminals rather than from the processing of the business system. Therefore, the accuracy, consistency, and other issues of data depend more on system design. For the data collected in IoT systems, there is often a trade-off between privacy protection and quality of service. Higher data accuracy will lead to better service quality, but it is more likely to be a disclosure of private information. Blurred data will reduce the quality of big data services, but it will better protect user privacy. Facing this problem, we are now looking for as much balance as possible, and in the future it may be solved by other technical means, such as encrypted data analysis.

Value: The value in IoT big data may not be homogeneous, and the value contained in a record may well be related to the state of the environment where it was created, or to the way services are designed and processed. For example, for a smart building system, the security sub-

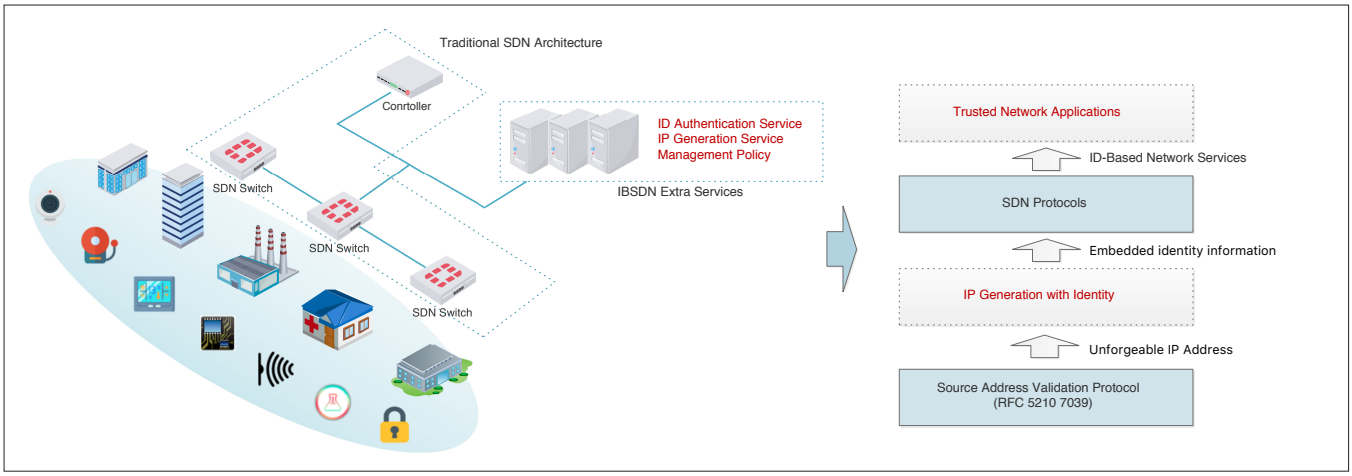

FIGURE 2. IBSDN architecture.

system may require all the real-time monitoring information, and each piece of data has value. But for a temperature control subsystem, the data obtained by random sampling at intervals is sufficient to support its services.

On the other hand, high-value IoT big data also provides new targets for potential cybercrimes [4, 15]. In the current rapid development of IoT applications, the common IoT security threats include the following.

Spoofing Attack

There are many types of spoofing attacks (e.g., ARP spoofing and DNS spoofing), and the most common in IoT systems should be IP address spoofing attacks. The purpose of this attack is to disguise malicious packets as legitimate ones so that they can be successfully processed in IoT systems. Such malicious attacks can be used in all IP-enabled IoT systems, where an attacker disguises itself as a legitimate terminal and then sends malicious data with a fake IP address to legitimize its own malicious actions, or to blame other innocent legitimate nodes for malicious actions [9]. In other IoT systems that do not support IP, there are similar attacks. For example, in an RFID environment, an attacker can counterfeit a valid RFID tag and then use a legitimate tag to generate a malicious packet that has been tampered with [8].

Resource Exhaustion Attack

IoT devices typically work in a resource-constrained environment such as energy, processing power, network bandwidth, and storage capacity. How to reduce resource consumption is an ongoing research hotspot in the field of IoT [1, 2]. In this case, an attacker can use unverified communication or service requests to consume a large amount of limited resources of the IoT device to launch an attack on certain nodes or the entire IoT network. The most common attacks include distributed denial of service (DDoS) attacks [7] and battery draining attacks [6].

Eavesdropping Attack

In the edge communication of IoT systems, wireless transmission technology is heavily used, and if data is transmitted unencrypted, an attacker can steal sensitive information, such as control instructions, credentials, and private data, in a way called eavesdropping or data sniffing. Eavesdropping also exists in traditional network environments, but in IoT systems more often use wireless communication, where terminal resources cannot always adopt a strong communication security mechanism, making it more vulnerable to eavesdropping attacks.

Malicious Application Attack

The biggest threats to the IoT application layer remain malware and worms. Compared to traditional network terminals, IoT terminals are quite different in single-device security capabilities; thus, malicious applications can easily destroy or control systems, resulting in the disclosure of private information or other threats to the proper operation of the system [5]. In the case of industrial production systems or medical systems, the consequences of these malicious applications can be severe. In addition, the ability of such malware to replicate itself makes it possible for them to extend the threat to other nodes and even form an attack path from IoT systems to the Internet.

Faced with high-value IoT systems and IoT big data, cyberattacks are still increasing. Unfortunately, traditional security mechanisms rely more on end-to-end devices or dedicated devices to provide network security, making them unsuitable to achieve desired results in such resource-constrained and highly heterogeneous IoT environments. For example, in larger IoT systems, traditional traffic filtering and firewall mechanisms may face potential scalability problems in this environment because gateway devices face resource constraints or heterogeneous challenges, which can lead to performance bottlenecks or single-point failures for the entire system. Another example is encryption protocols, where limited resources at IoT terminals severely limit the completeness and effectiveness of underlying encryption technologies. The situation requires novel network-based protection strategies to enforce security in a scalable and effective way.

The ID-Based SDN Architecture

Overview

The IBSDN architecture is based on the traditional SDN technology to increase the user identity recognition level for network traffic while achieving

network-side manageable and scalable security capabilities. IBSDN needs to deploy three network services in network management, namely terminal ID authentication service, IP address generation service, and management policy service, as shown in Fig. 2. The ID authentication service is used to identify the ID of the terminal user when accessing the network and determine its corresponding service authority. The IP address generation service is used to generate an IPv6 address embedded with identity information when the terminal is authenticated. The management policy server is used to store the latest management policies based on the identity of the terminal user, such as access rights and service priorities. Through the above services, all devices will perform identity authentication when accessing the network. Only through authentication can the network be properly accessed and the IP address embedded with its trusted identity information obtained. The controller in the SDN network can effectively monitor and manage all the traffic based on identity information by referring to the specific policies in the management policy server. IBSDN is based on the traditional SDN protocols and source address verification technology. First, source address verification technologies (e.g., RFC 5210 and RFC 7039) are used to ensure that the IP addresses of terminals in the deployment domain cannot be forged. Based on this, IBSDN designs an IP address generation mechanism that embeds terminal identity information to ensure that all network behavior can be traced at the packet level credibly. Later, using the traditional SDN network protocols, the network can be upgraded from address-based network management to identity-based network governance based on the identity information of the transmission flow, and finally provide support for trusted network applications from the level of network architecture.

Compared to the controller in the traditional SDN network, the additional information that the IBSDN controller needs to process is the mapping relationship between the IP and ID of terminals. Then the IP-based operations are upgraded to ID-based operations, for example, the generation of flow tables and management policies. Therefore, theoretically speaking, in the IBSDN network, a controller only needs to maintain an IP-to-ID mapping relationship in the management domain. Considering that the current controller is basically an independent server, the maintenance of this mapping table will not cause new bottlenecks in management and expansion for the controller.

For a terminal device or user, in the IBSDN network architecture, after accessing the network, there are three stages: identity authentication, obtaining an IPv6 address embedded with identity information, and performing identity tracing based on the IP address, as shown in Fig. 3. Specifically, when the terminal device accesses the network, it needs to perform authentication and normalization. In the IoT environment, it can be implemented by using a password or an identity certificate preset on the device. After the identity authentication, the IP generation service adds a timestamp to the ID information of the terminal, performs the encryption operation, generates the lower 64 bits of an IP address that

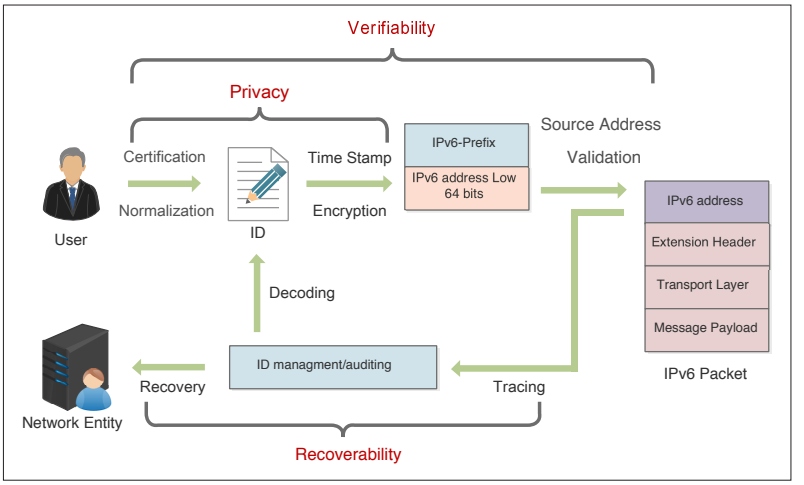

FIGURE 3. Flow of real identity in IBSDN.

is dynamically changed over time, and sends it to the terminal after the IPv6 address prefix is merged. Due to the source address verification technology, the IP addresses of all devices in the network cannot be forged. Under the protection of this technology, the IPv6 address of all devices in the network can be used as its own identity. At the same time, the private information of the device identity can be protected by the timestamp and encryption.

For network administrators, after obtaining the IPv6 data packets sent by the source terminal, the identity information of the terminal can be restored. Source ID management and traffic auditing can also be achieved by source IP decryption.

Devices ID Based on IPv6 Address

In the IBSDN architecture, we use the IPv6 address of the device as the identity. Specifically, we use the lower 64 bits of the address to indicate the identity of the terminal. There are two main issues that need to be addressed here. One is to protect the identity privacy of the terminal, and the other is to guarantee the authenticity of the address. First, we extend a user's existing ID (e.g., work permit number, student number, and ID number) to a 40-bit network ID, or NID for short. The extension method of the ID is not unique, and there may be multiple types. Which extension method is used in the current address is decided by a 1-bit extension type. After adding a 1-bit reserved bit and a 22-bit timestamp to form a 64-bit string, by encrypting (e.g., IDEA), we generate a 64-bit sddress ID, abbreviated as AID, and merge the AID with the current network address prefix, generating the final IPv6 address, as shown in Fig. 4. This series of operations will be done by the IP generation service within the domain and provide subsequent reverse decryption and identity traceback services. Through the ID information extension, timestamp splicing, and final cryptographic operations, the terminal's original identity information is protected from being intercepted by malicious users. It should be noted here that although the IP address of the terminal has been encrypted in IBSDN, for the forwarding device in the network, the terminal still has a valid IPv6 address. The encryption operation does not affect normal routing and forwarding. The pur-

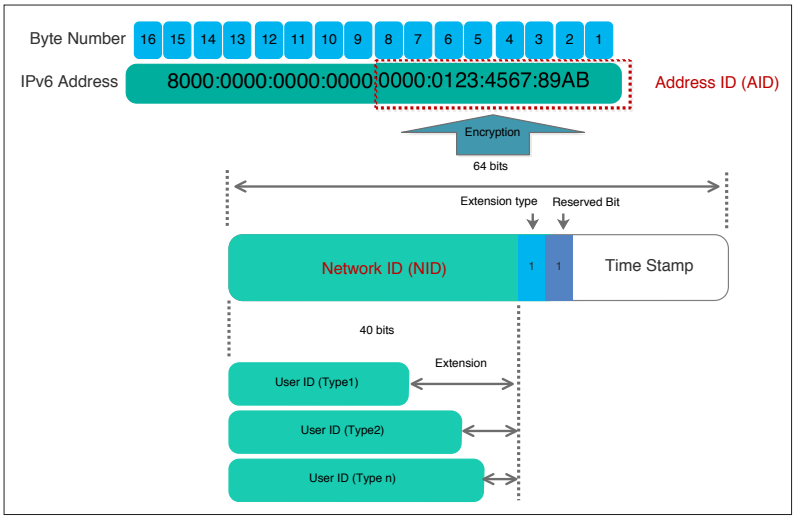

FIGURE 4. IPv6 address generation in IBSDN.

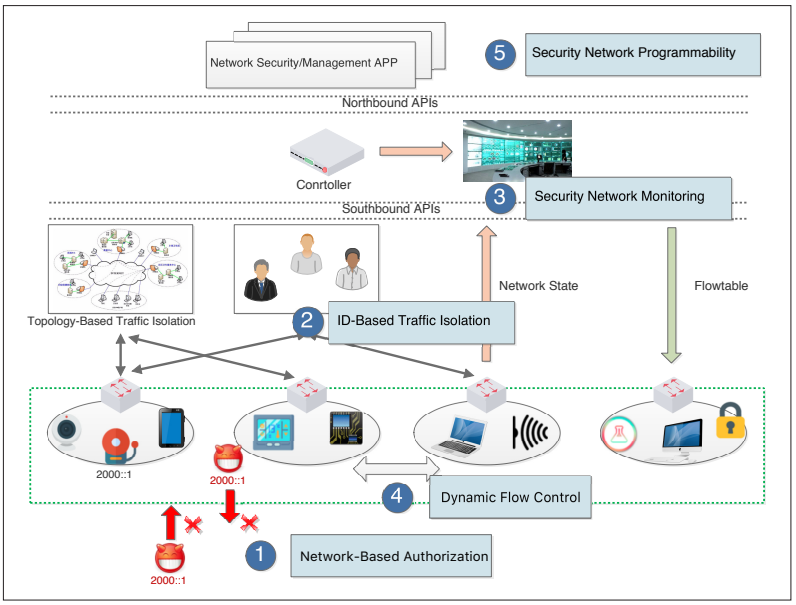

FIGURE 5. Security features of IBSDN.

pose of the encryption operation is to protect the identity information of the terminal hidden in the address.

The solution above needs to be established on the basis that the IP address of the network terminal cannot be falsified; hence, the IP address needs to be real and effective, which requires the support and guarantee of the source address verification technology. At present, there are mainly two kinds of solution to ensure the authenticity of the source address of the terminal device in the access network environment.

The first kind of solution is the source address verification technology. The main idea of this type of scheme is to establish a binding relationship between the network port and the corresponding IP address by listening to the network address request and allocating messages on the network device. The IP address of the terminal device cannot be forged.

The second kind is to use the 802.1X authentication scheme. After the terminal passes the 802.1x authentication, the terminal establishes a communication key between the access device and the terminal. This also ensures that the identity of the terminal device in the access network cannot be forged. Using the above scheme, a reliable network foundation with a real source address can be established for the identity embedding scheme in IBSDN.

Security Feature of IBSDN

The IBSDN architecture allows traditional SDNs to identify users and terminals. The granularity of this marking capability can be refined to the packet level. As shown in Fig. 5, this provides a more powerful management ability and improved security awareness for SDN, and it can better adapt to the complex and volatile environment of IoT. Next, we discuss in detail the security features that the IBSDN architecture may bring.

Network-Based Authorization: In IBSDN, the IP address of the network terminal cannot be counterfeited, and the identity information of the corresponding network entity is embedded in the IP address. Therefore, IBSDN gives the IoT system an autoimmune mechanism for malicious behaviors such as identity spoofing and address spoofing, which has formed an endogenous security capability. This ensures that the IoT devices in the deployment domain can rely on the identity-based trust mechanism provided by the network to implement trusted communication. Therefore, in a resource-constrained IoT environment, it is unnessary to redesign the peer identification mechanism on the terminals to ensure communication security. This should be helpful for IoT terminals that generally lack security defense capabilities. Similarly, IoT devices in the deployment domain cannot impersonate other IP addresses or identities to implement malicious network behaviors.

ID-Based Traffic Isolation

When we face high complexity in the network, virtualization is generally a solution that deserves serious consideration. The resource-constrained IoT environment also faces the difficulty of a high degree of network heterogeneity. The IBSDN architecture can implement ID-based slice partitioning and traffic logic isolation based on the traditional SDN slicing technology. This will bring more flexible and efficient solutions for network management and security defense for IoT systems, such as scenarios where user privacy is sensitive or has a high level of operational authority requirements.

Security Network Monitoring: The SDN network has wide control plane visibility that is unavailable in traditional networks, and it can provide network operation status information from data flow granularities. In IoT networks, there are a large number of terminal devices for monitoring and sensing. This type of device has the characteristics of low flow and high frequency in terms of network transmission. By embedding the terminal identity information in the IPv6 address, IBSDN can enhance the level of network monitoring from data stream to ID-based network behaviors, while avoiding the monitoring trap of low-flow high-frequency in the IoT scenario. At the same time, IoT monitoring based on network behaviors that can be compared with the normal network behaviors described by pre-defined rules or big

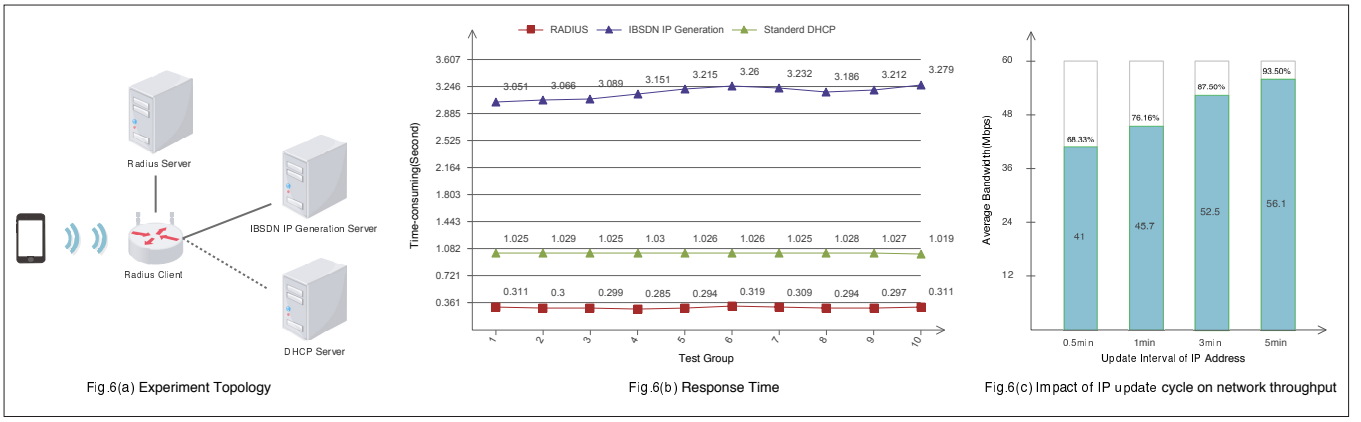

Fig.6(a) Experiment Topology

Fig.6(b) Response Time

Fig.6(c) Impact of IP update cycle on network throughput

FIGURE 6. Performance analysis of IBSDN.

data learning is also more helpful to discover the abnormality of the network security state or to sense potential attacks.

Dynamic Flow Control: A key feature of SDN is the separation of the data plane from the control plane. On this basis, the identity information is embedded in the network traffic, which enables the IBSDN controller to dynamically install or update the forwarding rules according to security policies or service requirements, and thereby manage traffic more appropriately. This enhanced manageability can significantly increase the potential of IoT to implement appropriate security mechanisms. In addition, dynamic flow control based on identity information can significantly increase potential countermeasures against security threats, not just blindly drop packets. These defense solutions may include dynamic isolation and network reflectors for advanced analysis or forensic analysis using honeypots.

Security Network Programmability: The enhanced network programmability provided by the SDN controller facilitates the development and deployment of network security applications. Furthermore, in IBSDN, since the controller can grasp the identity information of all data flows in the management domain, it makes it possible for IBSDN to provide a new group of development application programming interfaces (APIs) based on traffic identity for network security applications. This enables new applications in the IoT environment to establish security management policies based on the perception and analysis of network entity behaviors. This will undoubtedly make security applications more concise and efficient, and achieve better understandability and maintainability.

Performance Analysis

Based on the traditional SDN architecture, IBSDN establishes a real and reliable identity for the terminal, and it can improve the network management and security monitoring capabilities accordingly. In the IBSDN scheme, the terminal needs to perform identity verification when joining the network before generating an IPv6 address embedded with the terminal identity information. This process will consume more time than the traditional SDN architecture, resulting in efficiency decrease. After the address is generated, IBSDN's system performance is not significantly different from traditional SDN. Here we design two groups of experiments. The first one tests the address generation and delivery in IBSDN before comparing the time overhead of the standard DHCPv6 and discussing the performance of IBSDN. The other group of experiments tests the impact of the average bandwidth on different update intervals of IP address.

We set up the experimental topology shown in Fig. 6. A smartphone accesses the network through a wireless router. The wireless router communicates with the Radius server as a Radius client and verifies the identity of the terminal. In the first group of experiments, after measuring the time cost of obtaining the IPv6 address through the IBSDN IP generation server and through the standard DHCPv6, we conducted 100 experiments and obtained an average time cost every 10 times. The results are shown in Fig. 6, from which it can be found that the 100 experimental data fluctuations are not large. The maximum time for the IBSDN address generation service is about 3.279 s, with the lowest about 3.051 s and the average 3.174 s. The standard DHCPv6 maximum time overhead is about 1.029 s, the minimum is about 1.019 s, and the average is about 1.026 s. It can be found that since the address generation process of IBSDN requires the embedding operation of the terminal ID, the time overhead is almost three times that of the standard DHCPv6. Compared to the address generation service, the time cost of the Radius service is small, with an average of only about 0.302 s. Through experiments, it can be found that IBSDN causes more time overhead in the device access phase while bringing benefits such as security and trustworthiness, which means that the address generation service needs to bear about three times larger load than the traditional network environment, which needs to be considered in practical applications. On the other hand, because the IPv6 address of the terminal in IBSDN is embedded with a timestamp, the IP address will be dynamically updated at a certain interval, and the specific update interval can be set by the network administrator. In the second set of experiments, we focused on the communication efficiency of the network under different update intervals of IP address. We set the terminal to update the IP address at update intervals of 0.5 min, 1 min, 3 min, and 5 min, and continuously perform data transmission for 20 min on a link with a bandwidth of 60

Mb/s. Results are shown in Fig. 6, where it can be found that when the IP address is dynamically changed at an update interval of 0.5 min, the communication bandwidth of the terminal is significantly affected, and can only reach about 68.33 percent of the link bandwidth. As the time interval increases, the average bandwidth increases significantly. When the update interval is 5 min, it can reach 93.50 percent as the link bandwidth. According to the experimental results, in application scenarios where transmission efficiency is important, we recommend setting the dynamic update interval of IP to not less than 3 min, which can reach about 90 percent of the link bandwidth.

Challenges and Opportunities

Identity in Non-IP Environments: In the IBSDN architecture, we discuss the part of the IoT scenario that currently supports IP addresses, such as Wi-Fi, 6LoWPan, and Modbus. Although a large number of such devices exist in the IoT environment, there are still communication protocols that do not support IP, such as RFID and ZigBee. In the application scenario where IP is not supported, the existing solutions of IBSDN cannot be directly compatible. It is necessary to have an identifier mapping mechanism from IPv6 to the unique IDs of these protocols. In this identity mapping mechanism, it is necessary to have the identity recognition capability for the IoT device, ensuring that the mapping relationship cannot be forged.

The SDN Architecture in a Distributed Environment: The SDN architecture gains many competitive advantages from centralized design, such as manageability, efficiency, and programmability. However, when it faces a distributed scenario (e.g., cross-domain issues of multiple independent SDN management domains), its own congenital defects are also amplified, including IBSDN. At this point, designing a master controller that overrides all subnets is clearly not an acceptable option because the Internet itself is distributed. Therefore, we need to design a new overall architecture to solve this problem. Blockchain can be a potential solution. We can consider putting key information that affects cross-domain interaction and authentication into the blockchain and then use smart contracts to provide public authentication services. But the privacy protection and implementation efficiency issues involved need further research.

Conclusion

IoT and IoT big data have drawn the attention of researchers and commercial verticals in recent years. These two technologies, while actively improving the quality of people's lives, also bring new attack surfaces to potential cyber attacks. Compared to traditional networks, IoT networks are resource-constrained and highly heterogeneous. These features make traditional security solutions unsuitable for the IoT environment, thus requiring a network-based, scalable, and efficient security enhancement solution.

In this article, we first analyze the characteristics of the IoT big data and the potential security attacks. Then we propose an ID-based SDN security architecture called IBSDN. In this architecture, we use the powerful expression capability of IPv6 address while embedding the terminal identity information in it. With source address verification technology, the trusted and traceable device identity in the management domain is guaranteed. Finally, we analyze the security features of the IBSDN architecture and discuss the main challenges and opportunities in the future.

Acknowledgments

This work in this article was in part supported by the National Key R&D Program of China with No. 2018YFB0803405, the National Natural Science Funds for Distinguished Young Scholar with No. 61825204, the NSFC Project with No. 61932016, the Beijing Outstanding Young Scientist Program with No. BJJWZYJH01201910003011, the Beijing National Research Center for Information Science and Technology (BNRist) with No. BNR2019RC01011, the Huawei Technologies Entrustment Project with No.HF2019015003, the Key Research and Development Program for Guangdong Province (2019B010136001), and the Science and Technology Planning Project Guangdong Province LZC0023 and LZC0024, and the National Natural Science Funds with No. 61572278.

References

[1] X. Wang, K. Xu, and B. Mao, "GreenLink: An Energy Efficient Scatternet Formation for BLE Devices," *Wireless Commun. and Mobile Computing 2018*, 2018.
[2] X. Wang, K. Xu, and Z. Li, "Smartfix: Indoor Locating Optimization Algorithm for Energy-Constrained Wearable Devices," *Wireless Commun. and Mobile Computing 2017*, 2017.
[3] K. Xu *et al.*," Toward Software Defined Smart Home," *IEEE Commun. Mag.*, 2016, vol. 54, no. 5, pp. 116–22.
[4] A. R. Sadeghi, C. Wachsman, and M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," *2015 52nd ACM/EDAC/IEEE Design Automation Conf.*, 2015, pp. 1–6.
[5] I. Andre, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security Vulnerabilities and Challenges," *2015 IEEE Symp. Computers and Commun.*, 2015, pp. 180–87.
[6] M. H. R. Khouzani and S. Sarkar, "Maximum Damage Battery Depletion Attack in Mobile Sensor Networks," *IEEE Trans. Automatic Control*, 2011, vol. 56, no. 10, pp. 2358–68.
[7] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, 2017, vol. 50, no. 2, pp. 76–79.
[8] Y. Z. Li *et al.*, "Security and Privacy on Authentication Protocol for Low-Cost RFID," *2006 Int'l. Conf. Computational Intelligence and Security*, 2006, vol. 2, pp. 1101–04.
[9] A. Mukaddam *et al.*, "IP Spoofing Detection Using Modified Hop Count," *2014 IEEE 28th Int'l. Conf. Advanced Info. Networking and Applications*, 2014, pp. 512–16.
[10] H. Hu *et al.*, "Toward Scalable Systems for Big Data Analytics: A Technology Tutorial," *IEEE Access*, 2014, vol. 2, pp. 652–87.
[11] W. Fan and A. Bifet, "Mining Big Data: Current Status, and Forecast to the Future," *ACM sIGKDD Explorations Newsletter*, 2013, vol. 14 , no. 2, pp. 1–5.
[12] M. Hilbert, "Big Data for Development: A Review of Promises and Challenges," *Development Policy Review*, 2016, vol. 34, no. 1, pp. 135–74.
[13] T. Yu *et al.*, "Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things," *Proc. 14th ACM Wksp. Hot Topics in Networks*, 2015, pp. 1–7.
[14] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, 2010, vol. 54, no. 15, pp. 2787–2805.
[15] M. Shen *et al.*, "Secure SVM Training Over Vertically-Partitioned Datasets Using Consortium Blockchain for Vehicular Social Networks," *IEEE Trans. Vehic. Tech.*, vol. 69, no. 6, 2020, pp. 5773–83.

Biographies

Xiaoliang Wang received his Ph.D degree from the Department of Computer Science & Technology at Tsinghua University, Beijing, China, in 2017. Currently he is a lecturer in the

Information Engineering College at Capital Normal University. His research interests include wireless networks and network security.

Ke Xu [SM] received his Ph.D. from the Department of Computer Science & Technology at Tsinghua University, where he serves as a full professor. He has published more than 200 technical papers and holds 11 U.S. patents in the research areas of next-generation Internet, blockchain systems, the Internet of Things, and network security. He is a member of ACM. He has guest edited several Special Issues in IEEE and Springer journals. He is an Editor of the *IEEE IoT Journal*. He is Steering Committee Chair of IEEE/ACM IWQoS.

Wenlong Chen received his Ph.D. in communication and information systems from the University of Science and Technology Beijing, and currently is an associate professor at Capital Normal University. His research interests include network protocols, Internet architectures, high-performance routers, and IPv4/IPv6 transition.

Qi Li received his Ph.D. degree from Tsinghua University. Now he is an associate professor with the Institute for Network Sciences and Cyberspace, Tsinghua University. He has worked at ETH Zurich, the University of Texas at San Antonio, the Chinese University of Hong Kong, the Chinese Academy of Sciences, and Intel. His research interests are in network and system security, particularly in Internet security, mobile security, and big data security. He is currently an Editorial Board member of *IEEE Transactions on Dependable and Secure Computing* and *ACM Digital Threats: Research and Practice*, and has served on the organization or program committees of various premier conferences.

Meng Shen [M] received his B.Eng degree from Shandong University, Jinan, China in 2009, and his Ph.D degree from Tsinghua University in 2014, both in computer science. Currently he serves at the Beijing Institute of Technology, China, as an associate professor. His research interests include privacy protection for cloud and IoT, blockchain applications, and encrypted traffic classification. He received the Best Paper Runner-Up Award at IEEE IPCCC 2014.

Bo Wu received his Bachelor's degree from the School of Software at Shandong University, China, in 2014, and his Ph.D. degree from the Department of Computer Science and Technology at Tsinghua University in 2019. Currently, he works in the Network Technology Laboratory at Huawei Technologies. His research interests include network architecture, network security, and blockchain.