A Direct Anonymous Attestation Scheme Based on Mimic Defense MechanismTitle

Chen Yu， Liquan Chen， Tianyu Lu
Southeast University

二等奖

摘要

Machine-to-Machine (M2M) communication is a essential subset of the Internet of Things (IoT). Secure access to communication network systems by M2M devices requires the support of a secure and efficient anonymous authentication protocol. The Direct Anonymous Attestation (DAA) scheme in Trustworthy Computing is a verified security protocol. However, the existing defense system uses a static architecture. The "mimic defense" strategy is characterized by active defense, which is not effective against continuous detection and attack by the attacker. Therefore, in this paper, we propose a Mimic-DAA scheme that incorporates mimic defense to establish an active defense scheme. Multiple heterogeneous and redundant actuators are used to form a DAA verifier and optimization is scheduled so that the behavior of the DAA verifier unpredictable by analysis. The Mimic-DAA proposed in this paper is capable of forming a security mechanism for active defense. The Mimic-DAA scheme effectively safeguard the unpredictability, anonymity, security and system-wide security of M2M communication networks. In comparison with existing DAA schemes, the scheme proposed in this paper improves the safety while maintaining the computational complexity.

提出的方法

1. 框架

This paper combines the mimic defense idea with the DAA protocol to propose a Mimic-DAA scheme, and then an M2M mimic defense system, which attributes the problem of uncertain security threats to M2M network security to problems that can be solved by robust control theory and technology, thus ensuring secure access to M2M devices at the technical architecture level. The application scenario of the anonymous access scheme for M2M networks based on the mimic defense principle is shown in Fig. 1.

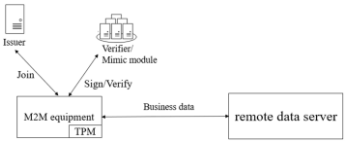

Fig. 1 M2M device communication scenarios

2. 实现过程

Mimic-DAA optimizes the original DAA scheme by introducing a two-attestation mechanism between the three parties and adding a mimic defense mechanism after the Verify phase. The improved process is shown in Fig. 3

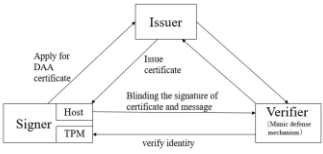

Fig. 2 Improved DAA protocol operation mechanism diagram

Because the core idea of the DAA protocol is to protect the anonymity of the platform and prevent the included protocol parties from being spoofed by the fake platform, existing DAA schemes always default to the Verifier's identity being legitimate, and the Verifier does not need to self-certify its identity. An attacker-controlled Verifier can receive the platform's signature information without restriction and then return the verified result without raising the platform's suspicion. However, in an M2M communication system, user data is the most important information for an attacker to focus on, and if the platform's signature is not verified and published, there is a high probability that it can be obtained and attacked. Therefore, in this paper, we add mimic security mechanisms to the DAA scheme and take the approach of verifying the platform by setting up multiple heterogeneous executors in a domain as part of the Verifier. Fig. 3 shows a typical dynamic heterogeneous redundancy architecture for a mimic defense system [13]. When there is a message input, it is transmitted to each heterogeneous executor in the heterogeneous pool through an input agent. All heterogeneous executors process the message and transmit the result to the multimode adjudication module, if the result is consistent, the output will be output; if not, an abnormality can be identified in the message output of an executor, thus realizing the security defense of the system.

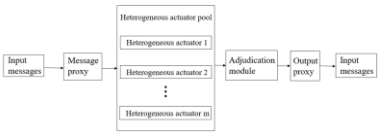

Fig. 3 Mimic defense system dynamic redundancy architecture diagram

The random number module generates a number of random numbers X1,X2,…Xn, which are encrypted and distributed to each group of heterogeneous executors, and each group of heterogeneous executors encrypts the encrypted random numbers as the number of each group. If the resulting random number is X1, first the random number module encrypts with its own key to get E(X1) , and then the heterogeneous actuator group encrypts it with its own key to get E(E(X1)), the above process is completed inside the Verifier and does not involve other communication objects. The above process is shown in Fig.4.

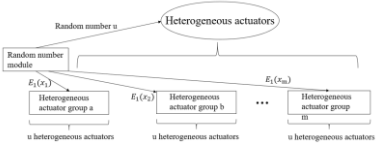

Fig. 4 Heterogeneous actuator grouping method diagram

实验

实验结果

Optimization of the DAA scheme: In the execution of attestation protocols, the main computations are focused on the exponential operations and bilinear mappings, so the analysis of efficiency should be measured by the amount of computation required to perform these two operations by the various entities involved in the protocol. The efficiency of the Mimic-DAA scheme is analyzed by comparing it with the schemes already proposed in the literature, as shown in Tables 1 and 2, both of which contain only the amount of computation required to perform each protocol in Mimic-DAA.

Table 1 Comparison of computational cost between parties in the Join phase

Stage	Scheme	TPM	Host	Issuer
Join	SC-DAA[14]	$3G_1$	$1G_1 + 2P$	$2G_1 + nG_1 + 1G_1^2$
	I-DAA[15]	$1G_1$	$2P$	$nG_1 + 1G_1^2$
	TMZ-DAA[16]	$4G_1$	0	$2G_1^2$
	Mimic-DAA	$2G_1$	$2G_1 + 1P^4$	$1G_1 + 1G_1^2$

Table 2 Comparison of computational cost between parties in the Sign/Verify phase

Stage	Scheme	TPM	Host	Verifier
Sign/ Verify	SC-DAA	$3G_1$	$3G_1 + G_T + 1P$	$2G_1 + 1G_1^2 + 2P + nG_1$
	I-DAA	$1G_1 + 1G_T$	$4G_1$	$1G_1^2 + 1G_2^2 + 4P + nG_1$
	TMZ-DAA	$3G_1$	$2G_1$	$2G_1^2 + nG_1$
	Mimic-DAA	$1G_1$	$6G_1$	$i(1G_1^2 + 1P^4 + nG_1)$

结论

This paper proposes an anonymous attestation method for M2M networks based on the mimic defense principle, applied in the scenario of device-to-device data communication within an M2M communication system. Firstly, the existing DAA scheme is optimized, and Verifier verifies the signature of the DAA certificate and the legitimacy of the platform after the platform is blinded. Also, because the Verifier identity is always legitimate by default, in order to prevent hijacking of M2M device access, a mimic defense mechanism is added to the Verifier side, using multiple dynamically redundant heterogeneous executors to form the attestation side, which can effectively defend against illegal third-party attacks. If the output of the heterogeneous executor is inconsistent when the adjudication module is working, it can also determine whether the heterogeneous executor is under attack and take effective defensive measures in time. The computational power requirements of the proposed scheme in this paper are high for mimic defense mechanisms, so subsequent work should continue to optimize the algorithm for mimic adjudication to conserve resources and expand the capacity of simultaneous access devices.

主要参考文献

[1] Y. Cao, T. Jiang and Z. Han, “A survey of emerging M2M systems: Context task and objective,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1246-1258, December 2016.
[2] B. S. Manoj, A. Chakraborty and R. Singh, Complex Networks: A Networking and Signal Processing Perspective, New Jersey, USA:Prentice Hall PTR, February 2018.

联系方式

联系人：Chen Yu
手机：15851813397
邮箱：792319313@qq.com