Lightweight PUF-Based Authentication Protocol for IoT Devices

Yildiran Yilmaz, Steve R. Gunn, Basel Halak
Electronics and Computer Science, University of Southampton, United Kingdom
E-mail: {yy6e14, bh9@ecs.soton.ac.uk}

INTRODUCTION

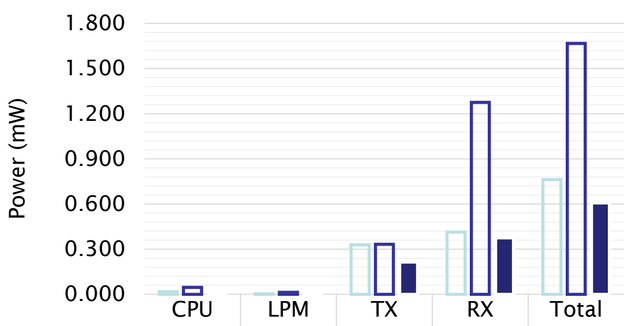
With the rapid growth and adoption of IoT, questions about security are being asked and rightly so. Some IoT applications deal with extremely sensitive data, and instructions. Imagine a scenario where sensors that detect moving objects in an autonomous vehicle is hijacked and made to send false reports to the breaking system; or a hijacked insulin pump, the attacker can alter the dosage of the of the insulin with fatal consequences. How about personal data from smart homes, and other body sensors, all these can lead to very disastrous consequences. Providing the fundamental information security guaranties of Confidentiality, Integrity and Availability is a major challenge for connected devices[1]. The main reason for this is the fact that these devices usually come constrained, they usually have very small ROM and RAM space, and processing capacity. These constraints make it impossible for conventional security protocols to be implemented on these devices, therefore new mechanisms have to be used to achieve security or modifications made to how the conventional protocols are implemented.

Several approaches have been taken in order to solve the security puzzle for constrained devices. Some of the approaches have built security on top of the Constrained Application (Protocol CoAP) using DTLS just like in [2]–[4], some have taken completely different route by using Physically Unclonable Functions(PUF) [5], [6]. The work proposes a new security protocol based on Physically Unclonable Functions.

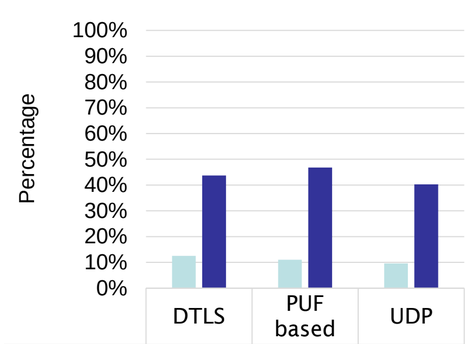
AIMS AND OBJECTIVES

The main objective of the proposed PUF model is to carry out the authentication between the verifier and prover without storing CRPs in the database. This is achieved by using a neural network model of the PUF. We masked the relationship between the challenge and the response by using RC5 algorithm to prevent adversary from collecting CRPs. We implemented this authentication method on windows platform using TCP connection in Csharp programming language and on resource constraint platform, which are contiki OS, Cooja and real resource constraint device: Zolertia remote, using UDP connection in C programming language. We have compared DTLS Implementation and proposed PUF based implementation on resource constraint devices considering RAM and ROM rrequirement, energy consumption by transaction, energy consumption in server and client side.

POWER CONSUMPTION AND MEMORY MEASUREMENTS



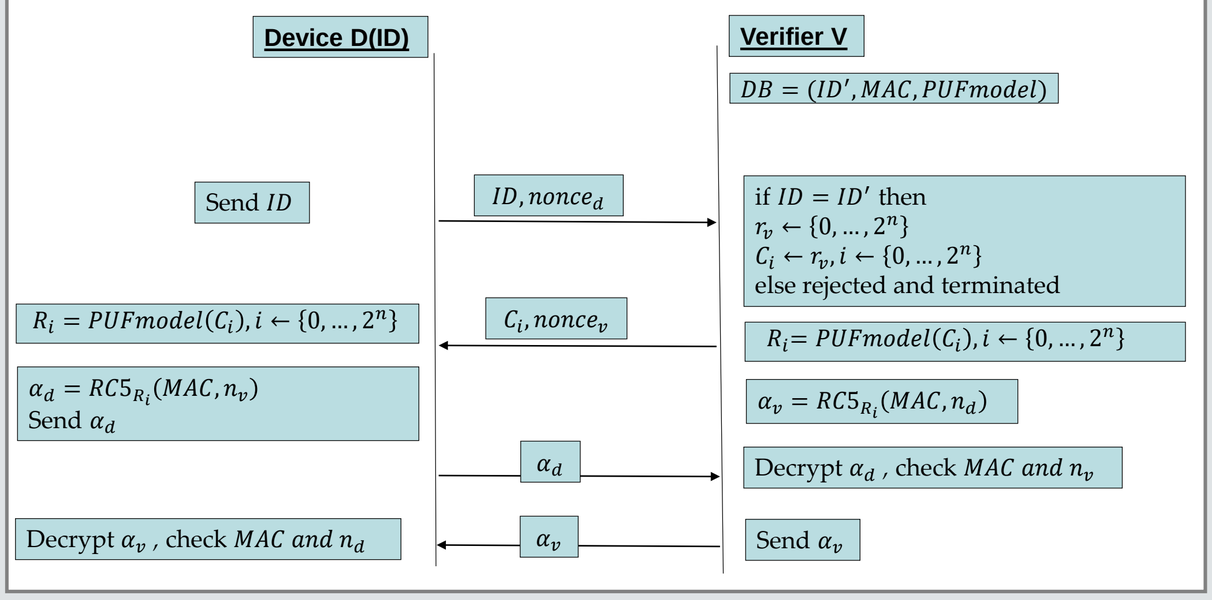
	CPU	LPM	TX	RX	Total
PUF based	0.017	0.003	0.329	0.413	0.762
DTLS	0.046	0.013	0.332	1.275	1.667
UDP	0.014	0.003	0.214	0.376	0.607



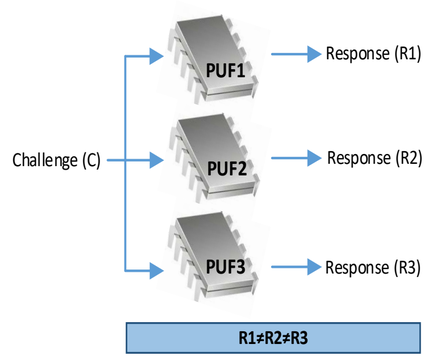
	DTLS	PUF based	UDP
Rom usage	12.52	11.01	9.63
Ram usage	43.74	46.84	40.26

[1] B. Halak, M. Zwolinski, and M. S. Mispan, 'Overview of PUF-Based Hardware Security Solutions for the Internet of Things', no. October, pp. 16–19, 2016.
[2] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, 'Lithe : Lightweight Secure CoAP for the Internet of Things', vol. 13, no. 10, pp. 3711–3720, 2013.
[3] A. Capossele, V. Cervo, G. De Cicco, and C. Petrioli, 'Security as a CoAP resource : an optimized DTLS implementation for the IoT', pp. 549–554, 2015.
[4] G. Lessa dos Santos, V. T. Guimaraes, G. da Cunha Rodrigues, L. Z. Granville, and L. M. R. Tarouco, 'A DTLS-based security architecture for the Internet of Things', in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 809–815.
[5] J. R. Wallrabenstein, 'Practical and Secure IoT Device Authentication using Physical Unclonable Functions', 2016.
[6] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, 'Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching', Proc. - IEEE CS Secur. Priv. Work. SPW 2012, pp. 33–44, 2012.
[7] F. Armknecht, R. Maes, A. R. Sadeghi, F. X. Standaert, and C. Wachsmann, 'A formal foundation for the security features of physical functions', Proc. - IEEE Symp. Secur. Priv., pp. 397–412, 2011.
[8] W. Liang, B. Liao, J. Long, Y. Jiang, and L. Peng, 'Study on PUF based secure protection for IC design', Microprocess. Microsyst., vol. 0, pp. 1–11, 2015.

PROPOSED PROTOCOL



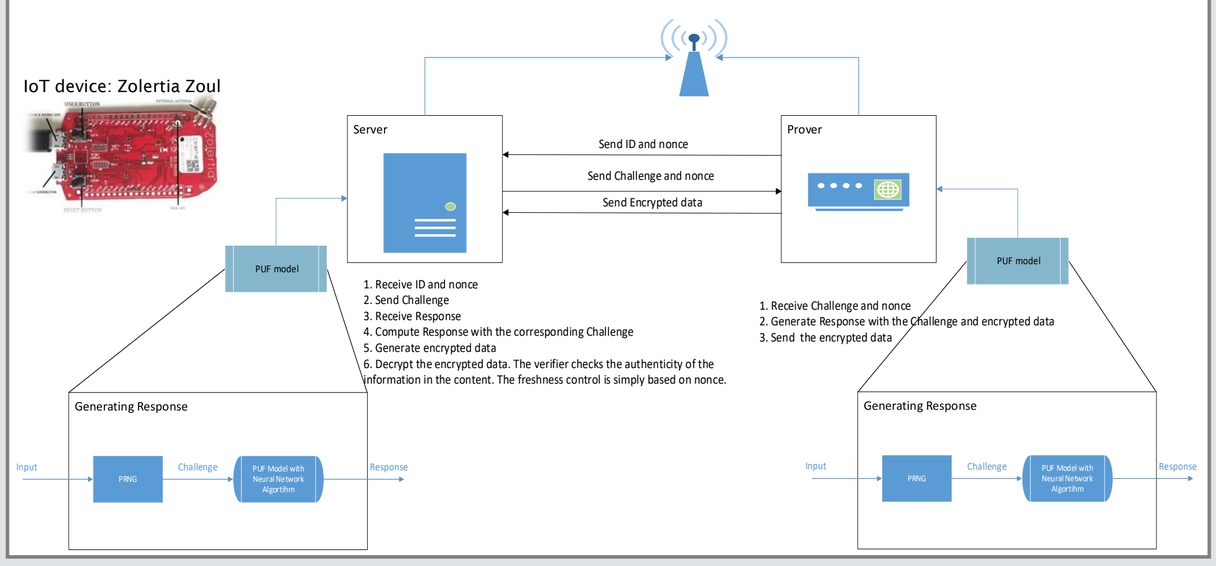
PHYSICALLY UNCLONABLE FUNCTIONS



Physical unclonable functions (PUF) are physical random functions that provide specific outputs for the physical objects they work in, which are simple to generate but practically hard to obtain without accessing the object. Many PUFs are proposed in the literature, however, not all are electronically implemented PUFs [7].

There are also many methods (optical, acoustical, compact disk, radio frequency, magnetic etc.) that have been implemented in many different ways. Electronic PUFs can be divided into three classifications: PUFs which exploit analogue electronic structures, delayed electronic components and memory elements[8]. Most of the PUFs, which are discussed in this work, utilise memory elements and the delays in the digital circuits, to generate unique outputs. They are also called silicon PUFs[8].

DETAILED VIEW: SERVER and CLIENT AUTHENTICATION



CONCLUSION

In conclusion, the proposed authentication protocol is more cost and time effective compared to DTLS handshake scheme and basic PUF authentication, since the system does not fill the database with millions of challenge-response pairs and the verifier computes the response via a PUF neural network model instead of a time consuming search of CRPs in a large database. The proposed authentication protocol is also resilient to cloning attacks, which is achieved by breaking the relationship between challenge and responses. We masked the relationship between the challenge and the response by using the RC5 algorithm. The RC5 algorithm hides the response. In this way, we hide real challenge and response pairs to prevent an adversary from collecting all CRPs and building a model of the PUF.

CENTRE FOR INTERNET OF THINGS AND PERVASIVE SYSTEMS

Author contact details
Email: {yy6e14, bh9@ecs.soton.ac.uk}
C-IoT Launch Event, 26 June 2018, Southampton