Authentication and Key Agreement Protocol for Ad Hoc Networks Based on the Internet of Things Paradigm

Muhamed Turkanović
University of Maribor, Faculty of Electrical Engineering and Computer Science, 2000 Maribor, Slovenia
CEI-Systems(.eu), Valvasorjeva ulica 10, 2000 Maribor, Slovenia, www.cei-systems.eu
E-mail: muhamed.turkanovic@gmail.com, m.turkanovic@cei-systems.eu
Tel: +386 40 303 874

Thesis summary

Keywords: authentication, key agreement, ad hoc networks, wireless sensor networks, internet of things

Received: February 22, 2016

The article summarizes the key findings of the doctoral thesis written by the author. The content of the thesis is based on the research fields of authentication and key agreement protocols (AKAP) for wireless sensor networks, and the internet of things (IOT). They key contribution of the thesis is a novel user AKAP for ad hoc networks, which is tailored for the IOT environment.

Povzetek: Prispevek predstavlja ključne rezultate doktorske disertacija avtorja. Vsebina disertacije temelji na raziskovlanima področjima protokolov za overjanje in dogovor o ključu (PODK) za brezžična senzorska omrežja in konceptu interneta stvari. Ključni prispevek disertacije je nov PODK za neinfrastrukturna omrežja, ki je prilagojen konceptu interneta stvari.

1 Introduction

The domain of ad hoc networks has gained an additional boost of attention in the last decade due to the increase of interest for the Internet of Things (IOT) paradigm. In the context of application scenarios inside IOT, security and privacy play a pivotal role. The issue with providing security and privacy inside IOT is the resource-constrained architecture (i.e., limited computational and communicational capabilities) of key devices like sensor nodes. As a solution the research community proposes lightweight protocols, which represent a trade-off between efficiency and security.

This paper presents a summary of a PhD Thesis [2] which focuses on lightweight authentication and key agreement protocols (AKAP) for ad hoc networks. The first part of the thesis reviews some existing lightweight AKAP for wireless sensor networks (WSN). It then presents a classification of possible attacks on AKAP for WSN, based on the analysis of existing protocols. Secondly with the help of the classification, an analysis of two novel and prominent AKAP for WSN [6, 1] was performed and the results concluded some flaws and shortcomings. Furthermore the first part encompasses the improvement of these schemes [4, 5].

The second part of the thesis focuses on proposing a new user AKAP for ad hoc networks, tailored for the IOT environment [3].

2 Proposed protocol

Numerous AKAPs for WSN have been proposed but very few have addressed the challenge of establishing a shared key in a secure and lightweight manner, between a sensor node and a user outside the WSN and from the IOT environment. In order to fill the gap and solve the problem, we developed a challenge-specific AKAP, which uses a rare four-step authentication model (Fig. 1), that we believe is the most appropriate for the mentioned scenario, where a remote user from the IOT wants to directly connect to a specific sensor node from a WSN.

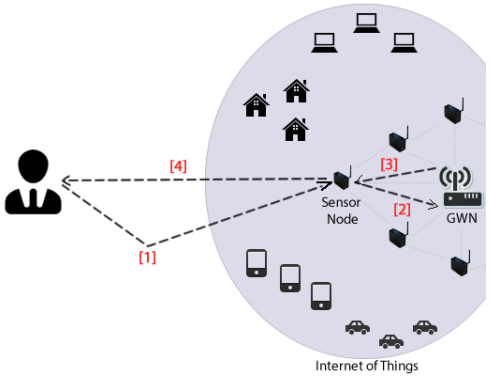

Figure 1: User authentication model of the proposed protocol [3].

Even though the protocols needs to be lightweight, be-

cause of the resource-constrained architecture of the sensor nodes, it still has to present the best possible trade-off between security and efficiency. The proposed protocol is thus based only on the use of simple mathematical computations as cryptographic hash functions and XOR. Furthermore, in order to lower the processing burden for the sensor node, the protocol uses the gateway node as a mediator for the authentication process. As a consequence, mutual authentication between all participants had to be implemented, since each participant has to be sure of the authenticity of the counterpart.

The protocol needs to be safe against all known and classified attacks against general AKAP and AKAP for WSN, thus we introduced the use of smart cards. Considering the protocol will be in use inside the IOT environment, it had also to be administrative- and user-friendly, thus enable dynamic node addition, enable the choosing and changing of user passwords, user anonymity etc.

3 Results and evaluation

After the development of the protocol, a security and performance analysis was performed. The security analysis was based on the ad hoc security model, which used the aforementioned classification of attacks. The results of the evaluation show that the protocol is resilient against all currently known attacks against general AKAP and AKAP for WSN.

The performance analysis consists of three separate evaluations, i.e. storage, communication and communication evaluation. The results of theses analysis show that the protocol is efficient, lightweight and thus suitable for resource constrained device like sensor nodes.

Furthermore, a comparison between the proposed protocol and other similar ones was performed. The results of the comparison show that the proposed protocol guarantees a higher level security than other protocols, while providing equal or better performance characteristics.

4 Conclusion

The paper summarizes the PhD Thesis [2], which addresses the problem of a user AKAP inside the IOT environment. The main contributions of the dissertation are:

- finding flaws and shortcomings in existing user AKAP for WSN;
- presenting a novel classification of attacks on user AKAP for WSN;
- development of improved versions of inadequate or deficient AKAP for WSN;
- development of a novel user AKAP for heterogeneous ad hoc WSNs based on the IOT paradigm.

The focus of further research will be the development a generalized protocol for the purpose of a more general use in the IOT. Moreover this protocol will not be based on the use of smart cards. We will also use the mathematical formal proof as a tool for the security evaluation of the proposed protocols.

References

[1] K. Das, Ashok, P. Sharma, S. Chatterjee, and K. Sing, Jamuna, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, p. 1646–1656, 2012.

[2] M. Turkanović, "User authentication and key agreement protocols for ad hoc networks, tailored for the internet of things environment," Ph.D. dissertation, University of Maribor, 2016.

[3] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[4] M. Turkanović and M. Hölbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Electronics and Electrical Engineering*, vol. 19, no. 6, pp. 109–116, 2013.

[5] M. Turkanović and M. Hölbl, "Notes on 'a temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks'," *Wireless Personal Communications*, vol. 77, no. 2, pp. 907–922, 2014.

[6] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, p. 316–323, 2013.