Poster Abstract: Lightweight Authentication Method for Controller Area Network

Ki-Dong Kang [1], Youngmi Baek [2], Seonghun Lee [3], Sang H. Son [1]
[1]Department of Information & Communication Engineering, DGIST, Daegu, Korea
[2]CPS Global Center, DGIST, Daegu, Korea
[3] Convergence Research Center for Future Automotive Technology, DGIST, Republic of Korea
{kd_kang, ymbaek, shunlee, son}@dgist.ac.kr

***Abstract*—In the age of smart and connected vehicles, there are significant issues in providing security for in-vehicle networking. Many security efforts for in-vehicle networks are still insufficient to build a lightweight security mechanism. Typically, it comes from the limitations of Controller Area Network (CAN) protocol common to in-vehicle network. We propose a lightweight authentication method based on one-way hash chain in CAN. In addition, we identify three technical challenges to be addressed for the proposed method and present our key idea to address them.**

Keywords-Controller Area Network; in-vehicle network security; authentication; Cyber-Physical Systems (CPS)

I. INTRODUCTION

These days, intelligent automotive cyber physical systems (CPS) have received great attention because of its promise as the means of next generation mobility. Although they offer excellent potential for road safety, convenience, and efficiency, they make an automotive system more complicated and increase the vulnerability. Especially, many researchers have demonstrated that a real vehicle could be attacked from anywhere by exploiting the various vulnerabilities of in-vehicle network for automotive systems [2, 3]. Controller Area Network (CAN) is the most common in-vehicle network for exchanging information among ECUs [1]. The sources of security vulnerabilities in CAN include: (1) no identification mechanism (no address of the sender and the receiver), and (2) a small payload size (maximum of only 8 bytes) to provide authentication. To counteract attacks on in-vehicle network, many authentication protocols have been proposed for CAN. However, it is essential for them to keep control of their overhead in terms of bandwidth utilization, processing time, or authentication delay. We propose to use a novel lightweight security protocol based on one-way hash chain, in order to provide the authentication in CAN.

II. AUTHENTICATION METHOD BASED ON HASH CHAIN

Lamport's authentication scheme where one-way hash chain is first used has been considered as one of classical lightweight authentication methods [4]. In our authentication protocol, we use the tip of one-way hash chain by inserting it into the extended ID field of data frame during transmission phase. Fig. 1 indicates a simple structure of data frame in CAN 2.0B protocol. The architecture of one-way hash chain is shown in Fig 2, and its tip value is utilized for source authentication.

ID	Extended ID	Data	CRC	ACK

Figure 1. Data frame of CAN 2.0B standard.

When we deploy an authentication method based on one-way hash chain for CAN, we should address several challenges.

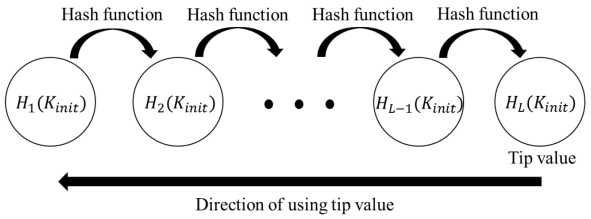

Figure 2. One-way key chain for source authentication.

There are three technical challenges to be addressed: (1) a limited length of hash chain, (2) securely sharing a seed with ECUs for re-initialization of hash chain, and (3) collision problem of one-way hash chain. They are due to limited resources of ECUs, broadcast nature of CAN, and small payload of CAN protocol, respectively. To address these challenges, we consider a tree based algorithm in our security protocol design.

III. CONCLUSIONS AND FUTURE WORK

We are developing a novel lightweight security protocol using one-way hash chain. In our effort, we focus on the technical challenges by assessing the feasibility of adopting the classical lightweight authentication method with one-way hash chain to CAN environment. We plan to address them by using a tree based algorithm. We expect that our lightweight authentication protocol will be more efficient when compared to existing authentication protocols while providing an sufficient authentication for CAN.

ACKNOWLEDGMENT

This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, DGIST Research and Development Program (CPS Global Center) funded by the MSIP, and Institute for Information & communications Technology Promotion (IITP) grant funded by the Korean government (MSIP) (No. B0101-15-0557, Resilient Cyber-Physical Systems Research).

REFERENCES

[1] R. Bosch. Can specification version 2.0. Rober Bousch GmbH, Postfach, 300240, 1991..

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In USENIX Security Symposium. San Francisco, 2011.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al. Experimental security analysis of a modern automobile. In Security and Privacy (SP), 2010 IEEE Symposium on, pages 447-462. IEEE, 2010.

[4] L. Lamport. Password authentication with insecure communication. Communications of the ACM, 24(11):770-772, 1981