Security in Integrated Vetronics: Applying Elliptic Curve Digital Signature Algorithm to a Safety-Critical Network Protocol-TTP/C

A. Deshpande*, O. Obi*, E. Stipidis*, P. Charchalakis*

**Vetronics Research Center, University of Brighton, Brighton, UK. BN2 4GJ.*

Corresponding author-a.deshpande@vetronics.org

Keywords: Safety, Security, TTP/C, ECDSA, Vetronics.

Abstract

Military vetronics consists of a variety of sub-systems which perform a myriad of functions. These sub-systems are connected together using gateways and backbone networks to provide the crew, the military and decision makers with real-time data, enabling information sharing. This integration of the vetronics architecture provides greater functionalities than an individual sub-system. However, this poses a potential risk from malicious attacks. For example, an attack on a safety-critical Drive-by-wire sub-system can affect the safety of the crew and compromise the mission. In this paper, we explore and carry out a feasibility study of applying elliptic curve digital signature algorithm on a safety-critical time-triggered protocol (TTP/C) to provide node authentication and message integrity.

1 Introduction

Integrated vetronics architectures in military vehicles consist of variety of command and control (C2) sub-systems such as safety-critical Drive-by-Wire (DbW) and weapons sub-systems, deterministic sub-systems (light control), and non-deterministic high bandwidth sub-systems (video for local situational awareness). These sub-systems are interconnected using gateways and backbone networks. Each individual sub-system consists of sensors/ actuators connected to individual electronic control units (ECU) and a communication network connecting all the ECUs to share data.

The use of integrated vetronics architectures provides the military with a cost effective approach in maintaining the fleet of vehicles throughout their life-span. This reduces the turnaround time during repair, enables the crew to perform reconfiguration tasks during the mission if necessary and incorporate real-time information sharing of mission critical data such as vehicle health, fire power, and situational awareness information eventually supporting mission success.

However, there lies a risk with the ubiquitous use of electronic devices, communication networks and interconnection of these networks within the vehicle from security attacks. [9]. Interconnection of safety-critical networks such as TTP/C with other sub-systems e.g. HUMS [6] exposes a security risk since the previously isolated safety-critical networks are now prone to attacks from these interconnections within the vehicle or from the outside through command, control, communications, computers and intelligence (C4I).

Consider a scenario where an ECU for safety-critical DbW sub-system is replaced when the vehicle is on a mission. The replaced ECU could contain a malicious code that triggers when the vehicle is operational and sends manipulated sensor readings to other ECUs causing an accident. Similar security attack can also occur from the outside world through the communication links to the vehicle. Hence, there is a need for stringent security techniques to be employed in vetronics.

Elliptic curve (EC) cryptography is a form of public key cryptography which provides RSA level security with a smaller key length. The technique is suitable for resource constrained environment and has been implemented on smart cards [22]. ECUs in safety-critical DbW sub-systems have limited resources for computation and hence application of cryptographic techniques in this environment is challenging.
In this paper we explore application of elliptic curve cryptography techniques and digital signature algorithm to achieve node authentication and message integrity on safety-critical network protocol TTP/C.

2 Related Work

Nolte, Hansson and Bello [13] describe different communication protocols used in automotive in-vehicle networks and explain the use of TTP/C protocol in safety-critical applications such as DbW. Nilsson and Larson [9, 10] perform simulated attacks on Controller Area Network (CAN), FlexRay and highlight that lack of security can affect the safety of the vehicle. Koscher Czeskis, Roesner, Patel and Tadayoshi [5] demonstrate the ability of an attacker to infiltrate a modern automobile's CAN through on-board diagnostic port. The authors also demonstrate gaining control of other sub-systems such as telematics through gateways and bridges. This threat can be catastrophic for military vehicles. Szilagyi and Koopman [15] explain the need for node authentication for CAN, FlexRay and TTP to protect against masquerade and replay attacks. The author highlights that TTP might be less vulnerable to such attacks however, with additional effort; an intruder can overcome the protocol characteristics to affect safety. The author also describes an authentication scheme for embedded multicast networks to protect against masquerade and replay attacks. The bandwidth overhead required by this scheme increases with the increase in number of nodes. Hence, this scheme is not suitable in military vetronics since certain safety-critical sub-systems can have large number of nodes. Wolf, Weimerskirch and Paar

[19] discuss variety of automotive bus systems and highlight the use of TTP in safety-critical applications such as DbW. The author describes attack scenarios and explains need for ECU authentication using a public key cryptography certificate based approach but doesn't describe any specific algorithm. Kleberger, Olovsson and Jonsson [3] identify lack of ECU authentication as a security problem within the in-vehicle network which can affect the safety. Wolf, weimerskirch and wollinger [20] explain the desired security properties for in-vehicle networks; introduce symmetric key, asymmetric key cryptography concepts for in-vehicle networks. The authors analyze the recommended key lengths for variety of cryptographic algorithms. We take inspiration from this analysis in further applying the concept of Elliptic Curve Digital Signature Algorithm (ECDSA) technique for vetronics. Paar [14] introduces core cryptographic concepts related to the in-vehicle network and discusses the computation overhead provided by public key cryptography techniques for their application in the in-vehicle network. Wollinger, Guajardo and Paar [21] describe implementation ECDSA asymmetric key cryptography algorithm on 16 bit 10-MHz microcomputer and conclude that it is possible to implement EC cryptosystems in highly constraint embedded systems environment. Bogdanov, Carluccio, Weimerskirch and Wollinger [1] describe variety of centralized and de-centralized architectures using security controllers for in-vehicle networks. Security controllers provide an expensive option to achieve security and add to the cost.

3 Problem Formulation

3.1 Time Triggered Protocol – TTP/C

The Vetronics Standards and Guidelines recommend the use of TTP/C for safety-critical sub-systems [2]. Hence, we use TTP/C as an example safety-critical network protocol in our work. TTP/C is based on time-triggered architecture (TTA) and uses time-division multiple access (TDMA) scheme [16]. Each node has an allocated time slot and sends the data packet onto the bus within that time slot which is broadcasted to all the other nodes connected onto the bus. This allows each node to fully utilize the full transmission capacity of the bus without any collisions. The sequence of TDMA time slots is called a TDMA round. Each node transmits data only once during each TDMA round.

TTP/C is organized as a set of conceptual protocol layers. The protocol layers group the related functions into one layer. The top most layer of the protocol stack is called as the host layer. The host layer contains application software running on a node. In a DbW sub-system the application software could be steering, braking or throttle. The underlying layers such as Fault-tolerant communication layer (FT-COM), protocol service layer, data link layer are all concerned with the safety aspects of the protocol and any modifications can lead to increased risk towards the safety functions of TTP/C [16]. We assume that if an intruder uses the TTP/C network for a security attack it could be through malicious or faulty application software. As a result we utilize the host layer in our approach. Figure 1 shows the TTP/C protocol layers.

TTP/C data frames consist of the data from the application software and can carry up to a size of 250 bytes per frame. Out of the 250 bytes of the frame 10 bytes are reserved for control values and 20 bytes for Cyclic Redundancy Check (CRC). Hence a TTP/C frame can take a payload from 2-236 bytes [18]. Depending on the node configurations within the cluster and the kind of application (e.g. steering, braking), nodes can send either single or multiple messages collectively up to 236 bytes. The CRC field uses checksum to detect transmission errors and does not provide any data integrity or authenticity.

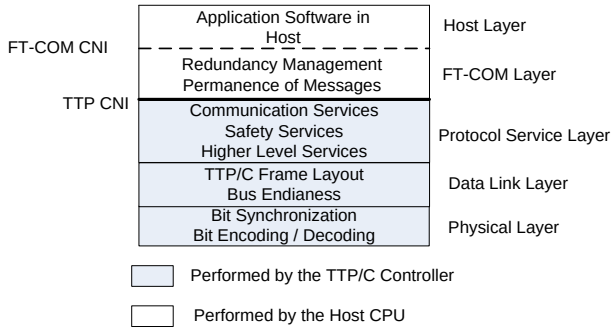

Figure 1: TTP/C protocol network layers.

4 Elliptic Curve Cryptography

Elliptic curve cryptosystems (ECC) were introduced independently by Neal Koblitz [4] and Victor Miller [8] in 1985. It is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. These kinds of cryptosystems can be viewed as elliptic curve analogues of the older discrete logarithm (DL) cryptosystems in which the subgroup of Z^*_p is replaced by the group of points on an elliptic curve over a finite field. For ECC based cryptosystems, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. This is known as the elliptic curve discrete logarithm problem (ECDLP) [7].

The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

4.1 Elliptic Curve Digital Signature Algorithm

The Elliptic Curve Digital Signature Algorithm (ECDSA) is an analogue of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography. ECDSA was first proposed in 1992 by Scott Vanstone [17] in response to NIST's (National Institute of Standards and Technology) request for public comments on their first proposal for Digital Signature Scheme. It was accepted in 1998 as an ISO (International Standards Organization) standard (ISO 14888-3), accepted in 1999 as an ANSI (American National Standards Institute) standard (ANSI X9.62), and accepted in 2000 as an IEEE (Institute of Electrical and Electronics Engineers) standard (IEEE 1363-2000) and a FIPS standard (FIPS 186-2).

Suppose an entity *A* wants to send a signed message *M* to an entity *B*. *A* hashes *M* (e.g. SHA-1) and signs the hashed message *H(M)* with its private key and sends the message, the encrypted hash and *H(M)* to *B*. On receipt, *B* verifies *H(M)* to make sure it has not been altered. *B* then verifies the signature using copy of *A's* public key. Figure 2 below illustrates this.

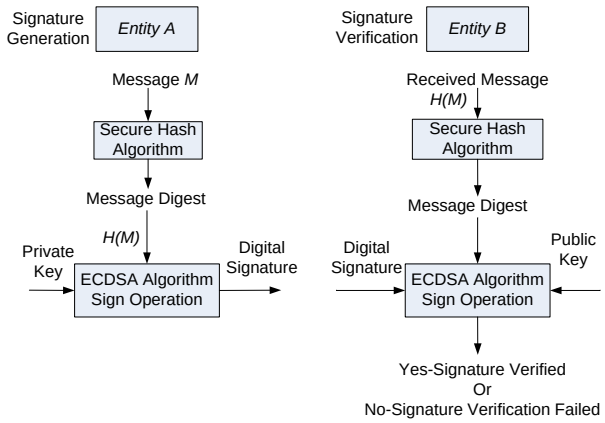

Figure 2: Block Diagram of Signature Generation/Verification Algorithm.

5 The Approach

Digital certificate based authentication for each ECU is recommended. This is because it facilitates providing most of the services (integrity, authentication, authorization and non-repudiation). A digital certificate is the means of associating an entity (in the case the ECUs) to a public key. This process is called binding. A certificate consists of the ECU identifier ID, the public key p*k* and the authorizations *Auth* of the respective nodes. Figure 3 below shows an example of a digital certificate.

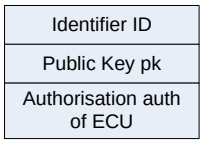

Figure 3: Digital Certificate

5.1 Node Authentication

Node authentication could be categorized in two parts. Authentication of all ECUs is needed to ensure that only ECUs with valid application software are able to communicate with safety-critical network system. Message authentication is needed to understand that the message sent is not malicious. All unauthorized messages may then be processed separately or are just immediately discarded. Therefore, it is assumed that every ECU has been flashed with secure firmware [11, 12] and has a certificate signed by the OEM to authenticate itself against the gateway as a valid ECU. When an ECU is powered on, replaced or repaired, the gateway verifies the OEM certificate and then proceeds with certificate generation and distribution required for message authentication.

The following activities occur when the driver powers on the vehicle and the engine starts running or when the vehicle is ready to move. Figure 4 below shows different states of the gateway in the authentication process. The gateway verifies the OEM certificate and generates public and private key pair. The ECUs also generate the public and private key pair and distribute their public keys to the gateway. The gateway stores the list of the ECUs public keys and distributes its own public key to all the ECUs in the network and also issues a certificate to other nodes to bind the nodes to their public key. The gateway signs the certificate using its secret key and the nodes verify the certificate using the gateway's public key.

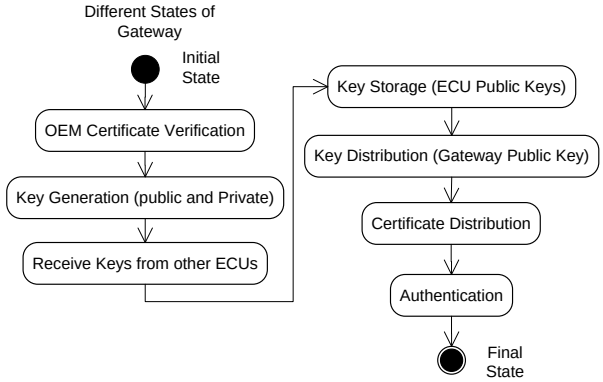

Figure 4: Different States of the Gateway

The ECUs use their private key to sign the message during each TDMA cycle of the TTP/C network. Figure 5 below shows the different states of the ECUs when transmitting and receiving a TTP/C message in every TTP/C cluster cycle. These states are based on use of ECC and a certificate based approach. The ECU or the TTP/C host uses the certificate and attaches the signature to every message before sending it onto the network. At the receiver side, the TTP host receives the message, verifies the digital signature using the certificate and accepts the message if the signature is valid.

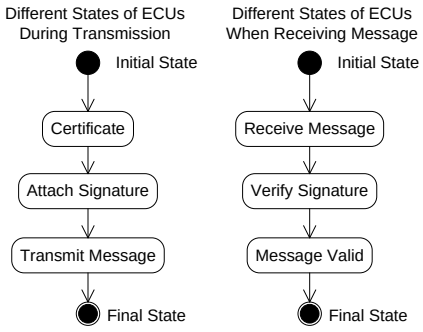

Figure 5: Different States of ECUs

6 Analysis

The use of elliptic curve cryptographic based authentication offers better efficiency over RSA because keys of shorter length can be used without the security of the system being compromised. In the ECDSA, the bits size of the public key required is twice the size of the security parameter, in bits.

Thus with a security parameter of 80 bits, the bits size of the public key is 160 bits [7]. Hence, an attack would require the equivalent of 2^80 signature generations per TTP/C message to discover the private key. It is worth noting that the security parameter less than 80 bits is insecure [7]. The size of the message hash, e.g. SHA-1 is 20 bytes [7] and the size of the digital signature is 4*t*bits, where *t* is the security parameter that would give a signature size of 320 bits for a security parameter 80 bits. The overhead created by employing the protection mechanism is 40 bytes, which leaves about 180 bytes of message space for a typical TTP/C node. Figure 6 below shows the performance of ECDSA through a schematic.

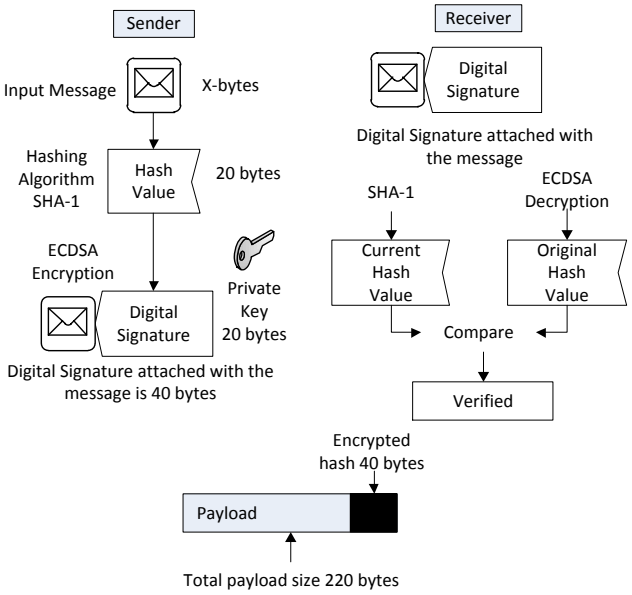

Figure 6: ECDSA performance for message authentication

The attractiveness of ECDSA lies in the fact that there is no sub exponential algorithm known to solve the ECDLP on a properly chosen elliptic curve. Thus, it takes full exponential time to solve the ECDLP compared to the RSA where the best known algorithms for solving the underlying integer factorization problem takes sub exponential time. This means that significant smaller parameters with equivalent security can be used in ECDSA than in RSA. Some benefits are faster computations, reduction in processing power, reduce storage space and bandwidth. This makes ECDSA very ideal for TTP. Below we give a table, comparing ECDSA key size with the RSA equivalent. Table 1 below shows key size comparison for ECDSA and RSA [21].

ECDSA	160	224	256	384	512
RSA	1024	2048	3072	7680	15360

Table 1: Key size comparison for ECDSA and RSA

7 Conclusion and Future Work

In this paper, TTP/C protocol is analysed and approach to node authentication and message integrity is presented. Use of OEM certificate to authenticate against the gateway provides node authentication. Node authentication prevents the attacker from getting access to the TTP/C global time base and thus preventing masquerading and reply attacks. In TTP/C, messages on the network can only be identified through the use of the protocol's global time base. Certificate based approach using ECDSA provides message integrity as well as identification of the source of the messages. This approach uses 40 bytes of available message payload for message signing leaving 180 bytes of payload for application messages such as steering, braking or throttle. The next step is to use modelling and simulation techniques to identify exact performance of the certificate based ECDSA approach.

Acknowledgements

This work is supported by the UK Ministry of Defence and TTTech.

References

[1] A. Bogdanov, D. Carluccio, A. Weimerskirch, T. Wollinger, "Embedded Security Solutions for Automotive Applications", *11th International Forum on Advanced Microsystem for Automotive Applications*, (2007).

[2] R. Connor, "VSI Vetronics Standards and Guidelines", *QINITEQ/EMEA/TS/CR0702540 Issue 3*, June (2009).

[3] P. Kleberger, T. Olovsson, E. Jonsson, "Security Aspect of the In-Vehicle Network in the Connected Car", *IEEE Symp. Intelligent Vehicles(IV)*, (2011)

[4] N. Koblitz, "Elliptic Curve Cryptosystems", *Mathematics of Computation 48*, pp. 203-209, (1987).

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, "Experimental Security Analysis of a Modern Automobile", *proc. IEEE Symp Security and Privacy*, (2010).

[6] J. Melentis, E. Stipidis, P. Charchalakis, F. Ali, "Towards a unified x-by-wire Solution with HUMS, HM and TTP: Lessons learned in implementing it to drive-by-wire vehicle", *16th International Conference on Real-time Network Systems*, (2008).

[7] A. Menezes, P. van Oorschot, S. Vanstone, "The Handbook of Applied Cryptography", *CRC Press*, (1997).

[8] V. Miller, "Use of Elliptic Curves in Cryptography", *Advances in Cryptology – CRYPTO 85*, Springer Lecture Notes in Computer Science, **Vol 218**, (1985).

[9] D. Nilsson, U. Larson, "Simulated Attacks on CAN Buses: Vehicle Virus", *Proceedings of the Fifth IASTED International Conference on Communication Systems and Networks*, pp66-72. (2008).

[10] D. Nilsson, U. Larson, F. Picasso and E. Jonsson, "A First Simulation of Attacks in the Automotive Network Communication Protocol FlexRay", *Proc. CISIS*, pp. 84-91.(2008).

[11] D. Nilsson, U. Larson, “Secure Firmware Updates Over the Air in Intelligent Vehicles”, *IEEE Conference on Communicaitons Workshops*, (2008).

[12] D. Nilsson, S. Lei, T. Nakajima, “ A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs, *IEEE GLOBECOM Workshops*, (2008).

[13] T. Nolte, H. Hansson, L. Bello, “Automotive Communications-Past, Current and Future”, *10th IEEE Conference on Emerging Technologies and Factory Automation EFTA*, (2005).

[14] C. Paar, “Embedded IT-Security in Automotive Application- An Emerging Area” In Embedded Security in Cars. *Springer Verlag*, ISBN 978-3-540-28383-4. (2006).

[15] C. Szilagyi, P.Koopman, “A Flexible Approach to Embedded Network Multicast Authentication”, *2nd Workshop on Embedded Systems Security (WESS)*, (2008).

[16] Time-Triggered Protocol TTP/C High Level Specifications Document Protocol Version v1.1, Document Number d-032-S10-028, Issued by TTTech.

[17] S. Vanstone, “Responses to NIST’s Proposal”, *Communications of the ACM 35*, pp. 50-52. (1992).

[18] A. Wasicek, C. El-Salloum, H. Kopetz, “ Authentication in Time-Triggered Systems using Time-delayed Release of Keys”, *IEEE Symp. Object/Component/Serive-Oriented Real-Time Distribution Computing (ISORC)*, (2011).

[19] M. Wolf, A. Weimerskirch, C. Paar, “Security in Automotive Bus Systems”, *Workshop on Embedded IT Security in Cars (ESCAR)*, Citeseer, (2004).

[20] M. Wolf, A. Weimerskirch, T. Wollinger, “State of Art: Embedding Security in Vehicles”, *EURASIP J. Emb. Sys*, (2007).

[21] T. Wollinger, J. Guajardo, C. Paar, “Cryptography in Embedded Systems: An Overview”, *Proc. Embedded World Exhibition and Conference*, pp. 735-744. (2003).

[22] A. Woodbury, D. Bailey, C. Paar, “Elliptic Curve Cryptogrpahy on Smart Cards without Coprocessors”, in *Fourth Smart Card Research and Advanced Application Conference*, Bristol, September 20-22, (2000). Kluwer.