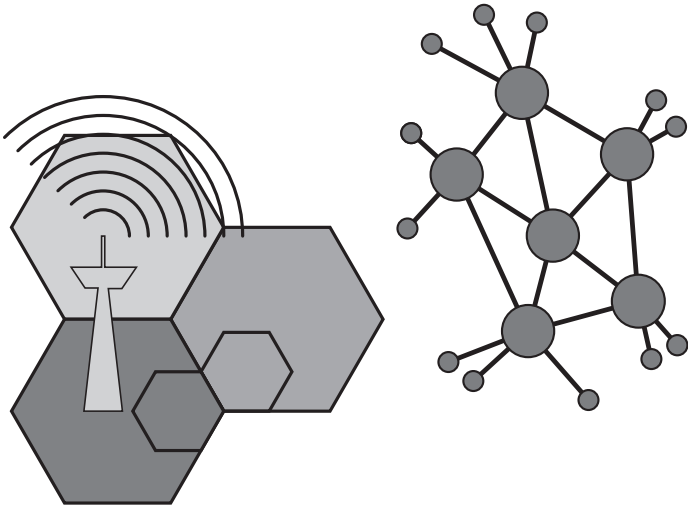
UNIVERSITÄT SIEGEN
Institut für Digitale Kommunikationssysteme

Forschungsberichte

Band 41 Herausgeber: Univ.-Prof. Dr. Christoph Ruland



**Venesa Watson**

# TSN-MIC - Message Integrity for Time-Sensitive Switched Ethernet Networks

**2021**

SHAKER VERLAG

# TSN-MIC - Message Integrity for Time-Sensitive Switched Ethernet Networks

DISSERTATION

zur Erlangung des Grades eines Doktors

der Ingenieurwissenschaften

vorgelegt von

MSc. Venesa Watson

geb. am 24. Dezember 1989 in Kingston, Jamaica

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät

der Universität Siegen

Siegen 2020

Betreuer und erster Gutachter

Prof. Dr. rer. nat. Christoph Ruland

Universität Siegen

Zweiter Gutachter

Prof. Dipl.-Ing. Dr.techn. Wolfgang Kastner

Technische Universität Wien

Tag der mündlichen Prüfung

14. Dezember 2020

**UNIVERSITÄT SIEGEN**

**Institut für**
**Digitale Kommunikationssysteme**

**Forschungsberichte**

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 41

**Venesa Watson**

# TSN-MIC - Message Integrity for Time-Sensitive Switched Ethernet Networks

SHAKER VERLAG

Düren 2021

**Bibliographic information published by the Deutsche Nationalbibliothek**
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Siegen, Univ., Diss., 2020



Printed in Germany.

ISBN 978-3-8440-7898-5
ISSN 1614-0508

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

*for it all begins with **You***

*Special thanks to Dr. Karl Waedt!*

# Abstract

Recent advancement in technology has seen the replacement of traditional analogue systems with their computer-based counterparts in manufacturing and industrial environments. Advantages realized from this change include increased functionality, flexibility, economy and reliability. Particularly with critical industries, there is reasonable concern regarding the significant risks to safety and security presented by the inclusion of these computer-based digital technology. The attack surface is further widened by the shift to connected infrastructures, such as the smart grid, driven by the Industry 4.0 (I4.0) and smart manufacturing industrial revolution, where Ethernet is proposed as the communication backbone. Specifically, it is the time-sensitive Ethernet variants, which have been integrated with additional services for time- and mission critical transmission, that have been earmarked for future infrastructures. Though Ethernet has the advantage of being a widely used standard that is compatible with a range of security controls, its performance makes it unsuitable for upholding the strict requirements for safety and security in critical environments. However, as a publicly available standard, the use of Ethernet, extended or otherwise, presents additional cyber-risks to critical environments.

The attack surface of Ethernet is considered in the context of critical industries, and a suitable security mechanism is proposed. In recent times, critical industries such as power plants and transportation services have been subjected to attacks that exploit message integrity to cause severe business disruptions and physical damage to critical infrastructure. As such, the proposal here is the implementation of an integrity preservation scheme, namely, the Time Sensitive Network – Message Integrity (***TSN-MIC***) scheme, which uses a lightweight algorithm for the preservation of message integrity. The main motivation for the ***TSN-MIC*** scheme, however, is to provide security at the lower OSI layers. Specifically, ***TSN-MIC*** is integrated at the OSI layer 2 to protect the TSN protocols, such as the time synchronization and TSN protocols that are implemented at the OSI layer 2. Existing security mechanisms particularly for manufacturing and industrial systems tend to target the upper OSI layers, and as such, do not provide protection against attacks at the lower layers. This leaves the time synchronization and the management services of the time-sensitive Ethernet/Time Sensitive Network (TSN) vulnerable. ***TSN-MIC*** is designed to be compatible with the different TSN specifications and to ensure negligible impact on their real-time performance.

***TSN-MIC*** not only provides integrity protection, but also includes mechanisms for online key change management and key change-over as a part of the key lifecycle for the session keys generated as a part of the ***TSN-MIC*** scheme. The proposed design of ***TSN-MIC*** is tested to prove its concept and to demonstrate its security and efficiency. Testing methodologies include software implementation using a Banana Pi (Bpi) R1 configured to operate as a switch and a laptop connected to act as an End System, which are used to validate the concept of the scheme, inclusive of the security feedback mechanisms. A software simulation of a TSN is made possible with OMNeT++ to demonstrate the efficiency of the proposed scheme. This simulation is implemented with the Avionics Full-Duplex Switched Ethernet (AFDX) protocol. The results of the tests indicate that ***TSN-MIC*** is suitably efficient, adding an average cost of **8.82%** in transmission time for each message from source End System to a destination End System, traversing a single switch between the source and destination. Through the Bpi R1 implementation, testing of the ***TSN-MIC*** security feedback mechanisms demonstrates that the scheme can detect and recover from faults that could affect the security and performance of the ***TSN-MIC*** scheme. This implementation further shows that the ***TSN-MIC*** scheme operates according to the design and successfully performs the cryptographic operations for integrity protection.

Further testing is required to demonstrate the viability of the scheme with different cryptographic algorithms implemented and to demonstrate its performance in different network designs. Nevertheless, it can be said that ***TSN-MIC*** serves as a suitable option for integrity protection for use in TSN networks, such as in critical infrastructure.

# Kurzfassung

Die jüngsten technologischen Fortschritte haben dazu geführt, dass traditionelle analoge Systeme in Fertigungs- und Industrieumgebungen durch ihre computergestützten Gegenstücke ersetzt wurden. Zu den Vorteilen, die sich aus diesem Wechsel ergeben, gehören erhöhte Funktionalität, Flexibilität, Wirtschaftlichkeit und Zuverlässigkeit. Besonders in kritischen Industrien gibt es begründete Bedenken hinsichtlich der erheblichen Risiken für die Sicherheit, die durch die Einbeziehung dieser computerbasierten digitalen Technologie entstehen. Die Angriffsfläche wird durch die Verlagerung zu vernetzten Infrastrukturen, wie z. B. dem intelligenten Stromnetz (Smart Grid), weiter vergrößert, die durch die industrielle Revolution der Industrie 4.0 (I4.0) und der intelligenten Fertigung vorangetrieben wird, wobei Ethernet als Kommunikations-Backbone vorgeschlagen wird. Insbesondere die zeitkritischen Ethernet-Varianten, die mit zusätzlichen Diensten für die zeit- und missionskritische Übertragung integriert wurden, sind für zukünftige Infrastrukturen vorgesehen. Obwohl Ethernet den Vorteil hat, ein weit verbreiteter Standard zu sein, der mit einer Reihe von Sicherheitskontrollen kompatibel ist, ist es aufgrund seiner Leistungsfähigkeit nicht geeignet, die strengen Anforderungen an die Sicherheit in kritischen Umgebungen zu erfüllen. Da es sich jedoch um einen öffentlich verfügbaren Standard handelt, stellt die Verwendung von Ethernet, ob erweitert oder nicht, zusätzliche Cyber-Risiken für kritische Umgebungen dar.

Die Angriffsfläche von Ethernet wird im Zusammenhang mit kritischen Industrien betrachtet und ein geeigneter Sicherheitsmechanismus wird vorgeschlagen. In jüngster Zeit waren kritische Industrien wie Kraftwerke und Transportdienste Angriffen ausgesetzt, die die Integrität von Nachrichten ausnutzen, um schwere Betriebsunterbrechungen und physische Schäden an kritischer Infrastruktur zu verursachen. Daher wird hier die Implementierung eines Integritätserhaltungsschemas vorgeschlagen, nämlich das Time Sensitive Network - Message Integrity (TSN-MIC) Schema, das einen leichtgewichtigen Algorithmus für die Erhaltung der Nachrichtenintegrität verwendet. Die Hauptmotivation für das TSN-MIC-Schema besteht jedoch darin, Sicherheit auf den unteren OSI-Schichten zu bieten. Konkret wird TSN-MIC auf der OSI-Schicht 2 integriert, um die TSN-Protokolle zu schützen, wie z. B. die Zeitsynchronisation und TSN-Protokolle, die auf der OSI-Schicht 2 implementiert sind. Bestehende Sicherheitsmechanismen, insbesondere für Fertigungs- und Industriesysteme, zielen in der Regel auf die oberen OSI-Schichten ab und bieten daher keinen Schutz gegen Angriffe auf den unteren Schichten. Dies macht die Zeitsynchronisation und die Managementdienste des zeitsensiblen Ethernet/Time Sensitive Network (TSN) angreifbar. TSN-MIC ist so konzipiert, dass es mit den verschiedenen TSN-Spezifikationen kompatibel ist und deren Echtzeitleistung nur geringfügig beeinträchtigt.

TSN-MIC bietet nicht nur Integritätsschutz, sondern beinhaltet auch Mechanismen für die Online-Schlüsselverwaltung und den Schlüsselwechsel als Teil des Schlüssel-Lebenszyklus für die Sitzungsschlüssel, die als Teil des TSN-MIC-Schemas erzeugt werden. Das vorgeschlagene Design von TSN-MIC wird getestet, um sein Konzept zu beweisen und seine Sicherheit und Effizienz zu demonstrieren. Die Testmethoden umfassen eine Software-Implementierung unter Verwendung eines Banana Pi (Bpi) R1, der als Switch konfiguriert ist, und eines Laptops, der als Endsystem angeschlossen ist, um das Konzept des Schemas einschließlich der Sicherheitsrückkopplungsmechanismen zu validieren. Eine Software-Simulation eines TSN wird mit OMNeT++ ermöglicht, um die Effizienz des vorgeschlagenen Schemas zu demonstrieren. Diese Simulation ist mit dem Avionics Full-Duplex Switched Ethernet (AFDX) Protokoll implementiert. Die Ergebnisse der Tests zeigen, dass TSN-MIC angemessen effizient ist und für jede Nachricht vom Quell-Endsystem zu einem Ziel-Endsystem, die einen einzigen Switch zwischen Quelle und Ziel durchläuft, durchschnittliche Kosten von 8,82 % in der Übertragungszeit verursacht. Durch die Implementierung von BPI R1 zeigt das Testen der TSN-MIC-Sicherheitsrückkopplungsmechanismen, dass das Schema Fehler, die die Sicherheit und Leistung des TSN-MIC-Schemas beeinträchtigen könnten, erkennen und beheben kann. Diese Implementierung zeigt außerdem, dass das TSN-MIC-Schema gemäß dem Entwurf funktioniert und die kryptografischen Operationen für den Integritätsschutz erfolgreich ausführt.

Weitere Tests sind erforderlich, um die Funktionsfähigkeit des Schemas mit verschiedenen implementierten kryptografischen Algorithmen zu demonstrieren und seine Leistung in verschiedenen Netzwerkdesigns zu zeigen. Nichtsdestotrotz kann gesagt werden, dass TSN-MIC als geeignete Option für den Integritätsschutz für den Einsatz in TSN-Netzwerken, z. B. in kritischen Infrastrukturen, dient.

# Contents