SHORT THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY (PHD)

SECURE COMMUNICATION PROTOCOLS

BY ÉVA CS. ÁDÁMKÓ

SUPERVISOR: PROF. ATTILA PETHŐ

UNIVERSITY OF DEBRECEN

DOCTORAL SCHOOL OF INFORMATICS

DEBRECEN, 2020

1 CONTENTS

2 SUMMARY

In the present dissertation, the vulnerabilities of two different communication methods were examined. The first one is the communication between the GPS satellites and receivers, and the second one is the communication between field devices in a Modbus RTU based SCADA system. The complete technical description is presented for both of the underlying systems. Example applications are given and described to show the broad applicability of both systems and to draw attention to how crucial it is to secure these communication flows. Vulnerabilities and security breaches are revealed by comprehensively studying the related scientific literature, and available solutions are presented for both of the examined systems. For the problem of securing the communication between GPS satellites and receivers, two solutions are made and given, with different level of provided security. For securing the communication between field devices in a Modbus RTU based SCADA system, one solution is designed and presented. Correctness check is implemented for the secure protocol created for GPS location calculation, and a test system is built to check the running parameters of the secure Modbus RTU communication.

3 RESULTS

2.1 FIRST THESIS POINT

The 3rd Section of the dissertation is devoted to revealing the security problems of different GNSS systems, especially the GPS, and overviewing the existing solutions for the disclosed security breaches by comprehensively examining the related scientific literature. Additionally, to give solutions for the revealed security problems and provide a way to authenticate location information from a cryptographical point of view.

2.1.1. REVEALING THE WEAKNESSES OF THE GLOBAL NAVIGATION SATELLITE

Even though the number of GNSS based services, especially the GPS based ones, has been increased enormously in the last decades, only a small part of the security issues of such systems got enough attention in the related scientific literature. Through these years the GNSS technology has gained a considerable portion in the civil, scientific, industrial, governmental, or military sectors, and the list is not complete at all. In Section 3.2.1 and 3.2.2 of the dissertation, the result of a comprehensive examination about the vulnerabilities of the American GNSS, i.e. the GPS is given. In the time of our research, it was the most popular, commonly used and stable GNSS system. Only a few information was available at that time in the related scientific literature about the cryptographic reliability of the entire GPS. On

the other hand, this approach is an essential part of the system, because there exist several GPS based service which has to provide cryptographically authenticated data, so it would be necessary to make location determination cryptographically secure and reliable. The research revealed that two types of threats could be distinguished, the ones that are attacking the geodetic authenticity of the system and the ones that are targeting the cryptographic authenticity of it. Geodetic authenticity can be threatened by intentional and malicious attackers through jamming and spoofing. Cryptographic authenticity is vulnerable because there can be no secure channel provided between the participants, so confidentiality, authenticity, data integrity, and freshness are not guaranteed parameters of the system. Geodetic weaknesses like jamming and spoofing are exhaustively examined in the related literature, and several solutions are performed. At the beginning of the 2000s, because of the widespread usage of GPS, several researchers started to design solutions for the cryptographical authentication shortcomings of the system too. A lot of possible methods were made, but it is important to mention, that all these solutions require fundamental changes in the structure of the GPS signals, so without the evolution of the system cannot be applied. **As a summary of my research, it can be stated that a solution which provides an authenticated location in a cryptographical sense and does not require fundamental changes in the structure of the GPS signal can be a niche (can be found in [1], [2]).** Security breaches of the GPS can be found in the following figure.

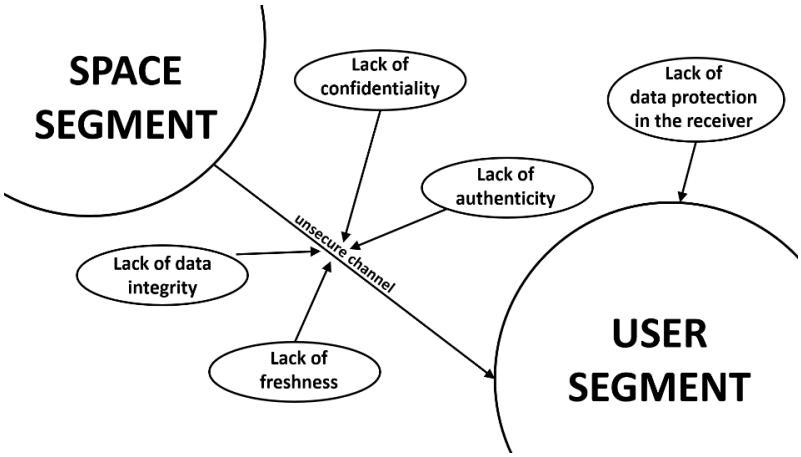


Figure 1. Security breaches of GPS

2.1.2. DESING AND REALISATION OF A „LOCATION-STAMPING" PROTOCOL ON THE SOFTWARE LEVEL

To solve the problem revealed in the first thesis point and provide cryptographically authentic location information without redesigning the GPS signal, two „location-stamping" protocols were made by my co-author and me in 2013 (can be found in

[2]). **The developed protocols can provide authentic location and time information for any device which has a GPS receiver built in it. The first solution provides safety with the help of a software component, a trusted third party, and a mobile phone service provider**. The aim of the above lower-safety solution, a.k.a the protocol built in the software level of the mobile device, is to provide a solution that is less hardware dependent. It can be done because it is much easier to access to the calculated GPS coordinates than to the Navigational Message broadcasted by the satellites. To authenticate the GPS information of the Mobile Device, a trusted third party is necessary, that is able to generate the location information of the Mobile Device. Then, the location information of the trusted third party can be compared to the ones received by the Mobile Device. One option to get suitable location information for comparison is to use mobile phone services, which provide cell information. However, cell information is not always accurate enough to specify the location of the Mobile Device. It is a proper solution if the mobile network coverage is broad enough. In the above situation, the mobile phone service has independent information on the location of the Mobile Device, which can be compared to the data that the Mobile Device has sent to the trusted third party. Exact steps of the protocol is described in Figure 2.

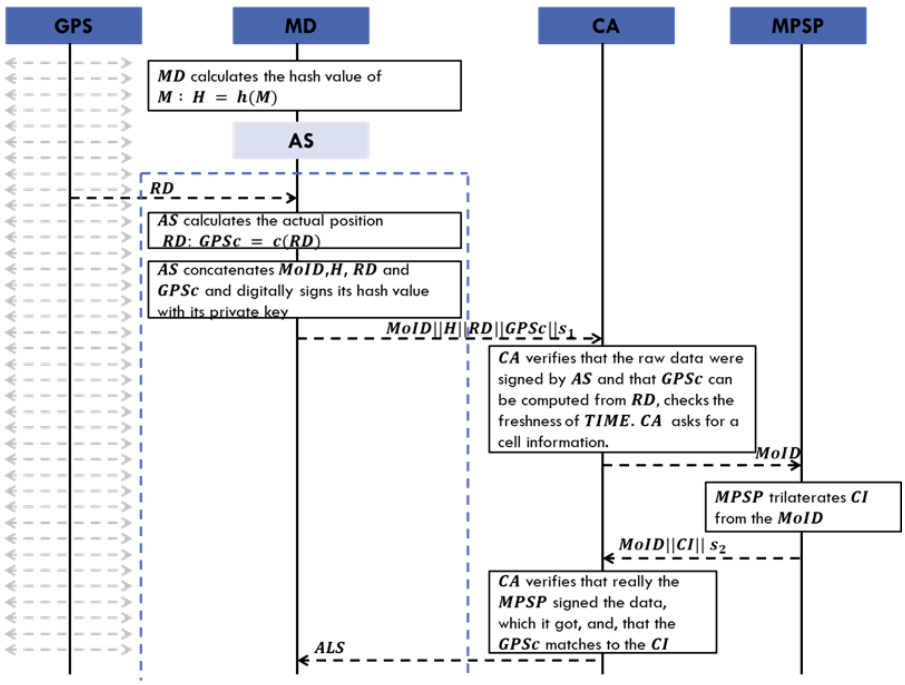


Figure 2. „Location-stamping" protocol on the software level

2.1.3. DESING AND REALISATION OF A „LOCATION-STAMPING" PROTOCOL ON THE HARDWARE LEVEL

The second solution provides higher-safety with the help of a software component and a trusted third party. **In this higher-safety solution, the main goal is to receive and preserve the content of the Navigational Message, transmitted by the satellites, before anybody could modify it (can be found in [2])** The Authentic Software is intended to be built in a very deep and hidden layer of the Mobile Device, namely in its driver level. The protocol, described in detail in Section 3.2.3.2 of the dissertation, has three important participants, which are the satellites of the Global Positioning System, the Mobile Device, and the Certification Authority. The designed higher-level protocol is built in a portable electronic device, which has been patented by the University of Debrecen in the US with the name "Portable electronic device, system, and method for authenticating a document associated with a geographical location" (can be found in [3]). Correctness proof was made with the Applied-π method, and the ProVerif software tool based on the events declared in the processes. The declared events label the steps of the protocol. The correspondence between the earlier declared events are investigated during correctness proof. The authenticity of the participants and the data integrity is proved by checking the correspondence assertions and injective correspondence for events of the subprocesses of the participants (can be found in [7]). Detailed steps of the designed protocol can be seen in Figure 3.

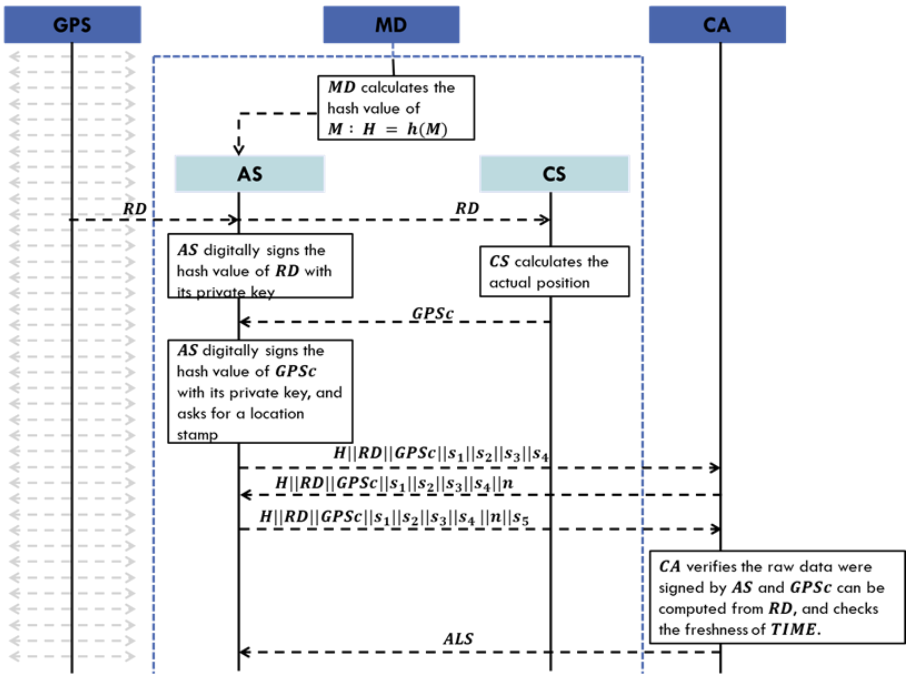


Figure 3. „Location-stamping" protocol on the hardware level

2.2 SECOND THESIS POINT

The 4th Section of the dissertation is devoted to uncovering the vulnerabilities of the Modbus RTU industrial communication protocol, which is one of the basic building blocks of such SCADA systems mentioned in Section 4.1.1.3. Additionally, to overview the existing solutions for the revealed vulnerabilities by comprehensively studying the related scientific literature, and to give a solution for the uncovered weaknesses from a cryptographical point of view.

2.2.1. REVEALED WEAKNESSES OF THE MODBUS PROTOCOL

Drinking fresh water, turning the lights on, travelling by tram, calling our family, or getting a medical treatment are usual activities. However, the underlying Critical Infrastructures which are maintained and controlled by the so-called "Supervisory Control and Data Acquisition systems" were always targeted by different types of attacks. During the last decades, because of the fast spread of internet-based services and continuous technical development, Critical Infrastructures become more vulnerable than ever, and cyberattacks happen more frequently. Consequences of such cyberattacks can be not only financial loss, or devastated reputation, but it can be extremely detrimental in health and safety. SCADA systems are often using outdated communication protocols, like the Modbus over Serial Line as an underlying network so that an update would be required. However, full reconstruction and innovative changes in legacy SCADA systems have a high cost, and it is not always possible to carry out. In this dissertation, the focus is on the Modbus protocol, especially the Modbus over Serial Line, a.k.a the Modbus RTU. The Modbus was originally designed and made by Modicon in 1979. The Modbus RTU protocol does not include any security considerations in default. During the design process, the required features of the Modbus protocol were reliability, speed, and accessibility, but the security of the used channel, thus authentication of the participants, confidentiality, data integrity, and freshness of the messages were left out, so not provided. **Our research – presented in Section 4.2.1 and 4.2.2 of the dissertation – addressed to find the vulnerabilities of a Modbus RTU based SCADA system by comprehensively reviewing the related scientific literature, and applying the Attack Tree method for summarizing and classifying the discovered security breaches (can be found in [4], [5], [6]).** Liabilities of Modbus RTU, revealed by us, are the lack of confidentiality, integrity, authentication, the sensibility for the Man in the middle attack, for Denial of Service Attack, the possibility of interception, interruption, modification, and fabrication. In the available literature, a proper solution for the abovementioned problems cannot be found in the case of Modbus RTU. Thus, the aims to be reached are to prevent the messages from eavesdropping, to authenticate the slaves and the master of the network, and to provide data

integrity and freshness of the messages sent via Modbus RTU. In Figure 4. the output of the attack-tree method is given.

2.2.2. DESING AND REALISATION OF A SECURE MODBUS RTU PROTOCOL

In Section 4.2.3 of the dissertation, our solution for the previously revealed vulnerabilities of the Modbus RTU protocol is presented. The solution is taken advantage of the fact, that the Modbus RTU based communication not always use its whole standardized message length and the messages have a relatively low update frequency. Usually, the Master Terminal Units and field devices have a built-in AES engine to encrypt the standard request and response before sending it. This engine is integrated by the device manufacturers and has no connection with the applied industrial communication protocol. However, the AES engine alone, with encrypting the messages before sent through the channel is not enough to solve all the revealed problems of the Modbus RTU protocol.

Our solution provides authentication of the participants to each other, and additionally data integrity, freshness, and confidentiality of the messages. A test system was designed and constructed in the Department of Electrical Engineering and Mechatronics at the University of Debrecen to check the applicability of the new solution (can be found in [8]). The running time of a single message exchange, applying our secure protocol, is five times longer than with the original Modbus RTU protocol. The overall performance of the device has not been reduced; all of its functionality has remained the same. Thus it can be stated that the protocol can be implemented in field devices also with low computational capacity. The results gained by applying our test system are the following: Time of generating a response on the slave side – initialization is not included – has increased with 400%. The time needed to transmit a response to the master has grown by 23%. Over the testing period, the rate of dropped messages was 1:15 000. Figure 5 and 6 displays the algorithm of communication with sensor slaves, and the designed test system.

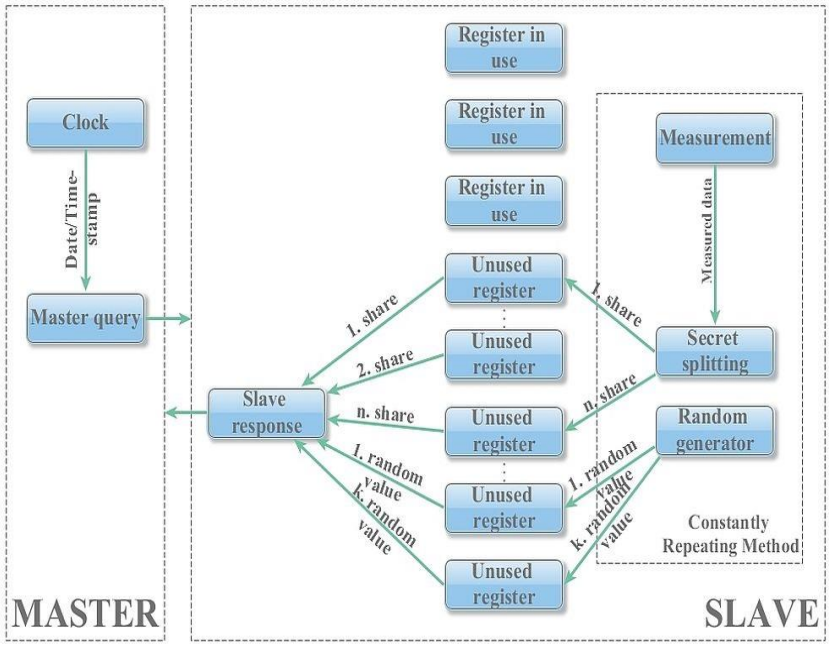


Figure 4. Secure Modbus RTU communication on the Sensor Slave side

UNIVERSITY of DEBRECEN

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/182/2020.PL
Subject: PhD Publikációs Lista

Candidate: Éva Csernusné Ádámkó
Neptun ID: TL4X9T
Doctoral School: Doctoral School of Informatics
MTMT ID: 10039859

List of publications related to the dissertation

Hungarian scientific articles in Hungarian journals (1)

1. Jakabóczki, G., Szemes, P. T., **Csernusné Ádámkó, É.**: A MODBUS RTU protokoll biztonságtechnikai vizsgálata, új kriptográfiai megoldások tesztelése = Security evaluation of MODBUS RTU protocol, testing new cryptographic methods.
   Int. J. Eng. Manag. Sci. 1 (2), 35-42, 2016. EISSN: 2498-700X.
   DOI: http://dx.doi.org/10.21791/IJEMS.2016.2.5.

Foreign language scientific articles in Hungarian journals (1)

2. **Csernusné Ádámkó, É.**: Security analysis of a "Location-stamping" protocol for GPS coordinates.
   Int. J. Eng. Manag. Sci. 2 (2), 1-12, 2017. EISSN: 2498-700X.
   DOI: http://dx.doi.org/10.21791/IJEMS.2017.2.1.

Foreign language scientific articles in international journals (4)

3. **Csernusné Ádámkó, É.**, Jakabóczki, G., Szemes, P. T.: Proposal of a Secure Modbus RTU communication with Adi Shamir's secret sharing method.
   Int. J. Elect. Telecomm. 64 (2), 107-114, 2018. ISSN: 2081-8491.
   DOI: http://dx.doi.org/10.24425/119357
4. **Csernusné Ádámkó, É.**, Jakabóczki, G.: Vulnerabilities of MODBUS rtu protocol?: a case study.
   Anale. Univ. Oradea. Fasc. Manag. Techn. Engin. 24 (1), 203-206, 2015. ISSN: 1583-0691.
5. **Csernusné Ádámkó, É.**, Szemes, P. T., Niitsuma, M.: Investigation on the heating system of the Mechatronics Research Center building using OLAP technology.
   Environ. Eng. Manag. J. 13 (11), 2733-2742, 2014. ISSN: 1582-9596.
   IF: 1.065
6. **Csernusné Ádámkó, É.**, Pethő, A.: Location-stamp for GPS coordinates.
   Acta Univ. Sap., Inf. 5 (1), 63-76, 2013. ISSN: 1844-6086.

Hungarian conference proceedings (1)

7. **Csernusné Ádámkó, É.**, Pethő, A.: "Helyszín-bélyegzés", hitelesített GPS koordináták.
In: Az elmélet és gyakorlat találkozása a térinformatikában II. : Térinformatikai Konferencia és Szakkiállítás Debrecen 2011. Szerk.: Lóki József, Debreceni Egyetem, Debrecen, 381-387, 2011. ISBN: 9789633181164

Foreign language conference proceedings (1)

8. **Csernusné Ádámkó, É.**, Jakabóczki, G.: Security analysis of Modbus RTU.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Szerk.: Kocsis Imre, University of Debrecen Faculty of Engineering, Debrecen, 5-11, 2015. ISBN: 9789634739166

Patents (1)

9. Bérczes, A., **Csernusné Ádámkó, É.**, Folláth, J., Pethő, A.: Portable electronic device, system and method for authenticating a document associated with a geographical location. 2013
Country: USA
Application Date: 2012.11.09
Registration number: US20130117572 A1-

List of other publications

Hungarian book chapters (1)

10. Bánóczy, E., **Csernusné Ádámkó, É.**, Husi, G., Piros, S., Szász, C., Szemes, P. T., Vitéz, A. C.: Épületmechatronika.
In: Fenntartható energetika megújuló energiaforrások optimalizált integrálásával. Szerk.: Kalmár Ferenc, Akadémiai Kiadó, Budapest, 119-166, 2014. ISBN: 9789630595407

Foreign language scientific articles in Hungarian journals (3)

11. **Csernusné Ádámkó, É.**: Online self-learning.
Int. J. Eng. Manag. Sci. 5 (1), 542-553, 2020. EISSN: 2498-700X.
DOI: http://dx.doi.org/10.21791/IJEMS.2020.1.44

12. **Csernusné Ádámkó, É.**: Gamification in programming: a short introductory session in programming with online games.
Int. J. Eng. Manag. Sci. 3 (5), 16-22, 2018. EISSN: 2498-700X.
DOI: http://dx.doi.org/10.21791/IJEMS.2018.5.2.

UNIVERSITY of DEBRECEN

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

13. **Csernusné Ádámkó, É.**, Szemes, P. T.: Evaluation of Consumer Behavior in the Building mechatronics research centre.
Recent Innovat. Mechatron. 1 (1-2), 1-5, 2014. EISSN: 2064-9622.

Hungarian conference proceedings (2)

14. **Csernusné Ádámkó, É.**: Játék alapú kódolás a középiskolában.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Imre Kocsis, Institute of English and American Studies, University of Debrecen, Debrecen, 5-10, 2017. ISBN: 9789634739814

15. **Csernusné Ádámkó, É.**, Szemes, P. T.: Az épületmechatronikai kutatóközpont szerepe a debreceni épületmechatronikai képzésben.
In: VIII. Energetikai konferencia 2013: 'Az energetika oktatása'. Szerk.: Szakál Anikó, Óbudai Egyetem, Budapest, 35-40, 2013. ISBN: 9786155018923

Foreign language conference proceedings (3)

16. **Csernusné Ádámkó, É.**: Online Self-Learning Methods for Programming.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Kocsis Imre, University of Debrecen Faculty of Engineering, Debrecen, 4-7, 2020. ISBN: 9789634901747

17. **Csernusné Ádámkó, É.**: Comparative analysis of project-based programming courses in Hungarian and foreign classes.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Imre Kocsis, University of Debrecen Faculty of Engineering, Debrecen, 5-12, 2016. ISBN: 9789634739456

18. **Csernusné Ádámkó, É.**: Design and Correctness Proof of Cryptographic Protocols.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Kocsis Imre, University of Debrecen Faculty of Engineering, Debrecen, 4-9, 2014. ISBN: 9789634737612

Total IF of journals (all publications): 1,065
Total IF of journals (publications related to the dissertation): 1,065

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

10 June, 2020

DOKTORI (PHD) ÉRTEKEZÉS TÉZISEI

BIZTONSÁGOS KOMMUNIKÁCIÓS PROTOKOLLOK

CSERNUSNÉ ÁDÁMKÓ ÉVA

TÉMAVEZETŐ: DR. PETHŐ ATTILA

DEBRECENI EGYETEM

INFORMATIKAI TUDOMÁNYOK DOKTORI ISKOLA

DEBRECEN, 2020

1 ÖSSZEFOGLALÁS

Kutatómunkám során két különböző kommunikációs folyamat sebezhetőségét vizsgáltam kriptográfiai szempontból. Az első kommunikációs folyamat a GPS (Global Positioning System) rendszerben, a GPS műholdak és a GPS vevőkészülékek között valósul meg. Ebben az esetben a célom a vevőkészülék GPS koordinátákkal adott földrajzi helyének kriptográfiai hitelesítése volt. A második kommunikációs folyamat a SCADA (Supervisory Control And Data Acquisition) rendszerekben, a rendszer terepi eszközei között valósul meg a Modbus RTU (Remote Terminal Unit) ipari kommunikációs protokoll segítségével. Itt a célom a terepi eszközök közötti biztonságos kommunikációs csatorna létrehozása volt, vagyis a résztvevők hitelesítésének, valamint az üzenetek bizalmasságának, integritásának és frissességének biztosítása volt. Mindkét esetben olyan megoldást kerestem, amely a kommunikáció alapjául szolgáló rendszerek fizikai struktúráját és adatátviteli keretét nem érinti. Dolgozatomban a vizsgált rendszerek működési alapelveit részletesen tárgyalom, majd példákkal szemléltetem a rendszereken alapuló különböző szolgáltatásokat, így megmutatva az általam vizsgált kommunikációs folyamatok kriptográfiai biztonságának alapvető fontosságát. A GPS-műholdak és vevők közötti kommunikáció biztonsági problémájának kiküszöbölésére két megoldást (protokollt) adtunk szerzőtársammal, amelyek különböző szintű kriptográfiai és/ vagy geodéziai védelmet biztosítanak. Ezek közül az egyik protokoll helyességének bizonyítása is megtörtént. A terepi eszközök közötti kommunikáció kriptográfiai védelmére egy megoldás adtunk, illetve megépült egy SCADA rendszer az elkészült protokoll futási paramétereinek és használhatóságának tesztelésére.

2 EREDMÉNYEK

2.1 ELSŐ TÉZISPONT

A disszertációm harmadik fejezete a különböző GNSS rendszerekkel, ezek közül elsősorban a GPS rendszerrel kapcsolatos eredményeimet ismerteti. Egy átfogó irodalomkutatás és feldolgozás során feltártam a GPS rendszer biztonsági problémáit mind geodéziai, mind kriptográfiai szempontból, valamint áttekintettem és elemeztem a megtalált biztonsági hiányosságok kiküszöbölésére már létező megoldásokat. Szintén ebben a fejezetben mutatok be két, a szerzőtársammal közösen készített „Helyszín-bélyegző” protokollt, amelyekkel a hiányzó biztonsági paraméterek okozta problémák kiküszöbölhetőek. **Ezekkel a protokollokkal a GPS rendszer által szolgáltatott helyadatok kriptográfiai szempontból hitelesen és letagadhatatlanul hozzárendelhetőek egy adott vevőkészülékhez**. **Az első**

tézispont a GPS rendszer hiányosságainak feltárását, valamint a két „Helyszín-bélyegző” protokoll (az egyik szoftver a másik hardver szintre integrált) tervezését és megvalósítását tartalmazza.

2.1.1. A GPS RENDSZER HIÁNYOSSÁGAINAK FELTÁRÁSA

A GNSS-alapú szolgáltatások gyakoriak polgári, tudományos, ipari, kormányzati vagy katonai alkalmazásokban, számuk az elmúlt néhány évtizedben rendkívüli mértékben nőtt. Ennek ellenére a kapcsolódó szakirodalom a GNSS rendszerek biztonsági hiányosságainak csak egy szűk szegmensével foglalkozik. A 3.2.1. és 3.2.2. fejezetekben az amerikai GNSS, azaz a GPS rendszer hiányosságait feltáró vizsgálataimat, és azok eredményét ismertetem.

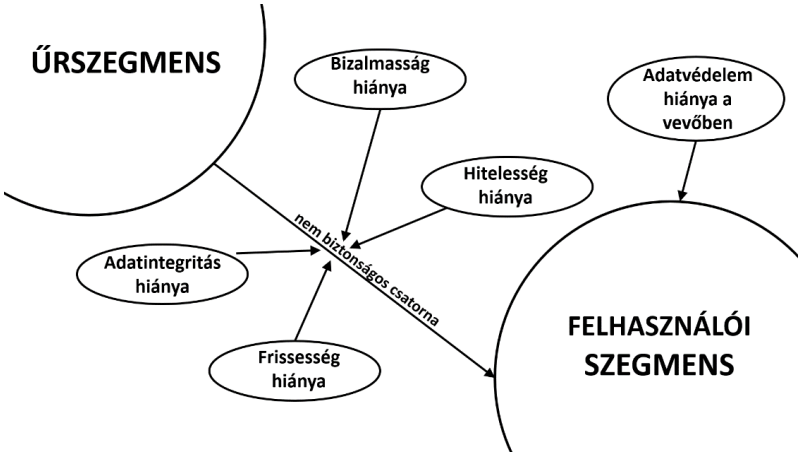
Kutatásunk idején a GPS volt a legnépszerűbb, leggyakrabban használt, legnagyobb lefedettségű és a legstabilabban működő GNSS rendszer, mégis csak igen kevés információ állt rendelkezésre a GPS rendszer kriptográfiai biztonságáról. Pedig számos olyan GPS-alapú szolgáltatás létezett és létezik ma is, ahol elengedhetetlen, hogy a helymeghatározás kriptográfiai szempontból is biztonságos legyen. Dolgozatomban azon szolgáltatásokkal foglalkoztam, ahol a GPS koordinátáknak valamely jogi eljárásban bizonyító ereje van.

A GPS rendszer két szempontból is sérülékeny: geodéziai és kriptográfiai hitelessége is sérülhet egy rosszindulatú támadás során. A geodéziai szempontból hiteles helymeghatározást veszélyeztető támadások két típusa a „Zavarás” és a „Megtévesztés”. „Zavarás” esetén a támadó – a GPS jel elfedésével – a teljes szolgáltatást elérhetetlenné teszi a GPS vevő számára, míg „Megtévesztés” esetén a valóstól eltérő helyadatokkal téveszti meg azt. Ezen támadások azért kivitelezhetőek, mert a műholdak által sugárzott jel a földfelszín közelébe érve már jelentősen gyengül. Az fenti támadástípusok elhárítására több módszer is ismert, amelyeket a vonatkozó szakirodalom részletesen tárgyal.

Kriptográfiai szempontból más a helyzet, mivel a műholdak és a vevők közötti kommunikációs csatorna nem rendelkezik az alapvető biztonsági jellemzőkkel: nevezetesen az üzenetek bizalmassága, integritása és frissessége, valamint a résztvevők hitelessége sem garantált. Emellett a vevőkészülékek sem tekinthetők kriptográfiai szempontból megbízhatónak, mivel az általuk fogadott adatok, vagy az általuk számított koordináták nincsenek megfelelően védve a rosszindulatú módosításoktól. A 2000-es évek eleje óta folynak kutatások a rendszer kriptográfiai hiányosságainak pótlására. Több módszer is született, de ezek kivétel nélkül alapvető változtatásokat igényelnek a GPS-jel szerkezetében, tehát a rendszer átalakítása nélkül nem alkalmazhatóak.

Összefoglalva elmondható, hogy olyan eljárás, amely nem igényel alapvető változtatásokat a GPS-jel szerkezetében, és amely kriptográfiai értelemben hitelesíti a helymeghatározást, azaz biztosítja az üzenetek bizalmasságát, integritását, frissességét, valamint a résztvevők hitelességét, emellett a vevőkészülékekhez hitelesen és letagadhatatlanul hozzárendeli az általuk számolt GPS koordináták által adott helyet és időt, a vizsgálataim előtt nem állt rendelkezésre. (lásd[1],[2])

Az általam feltárt biztonsági hiányosságokat a következő ábra foglalja össze.

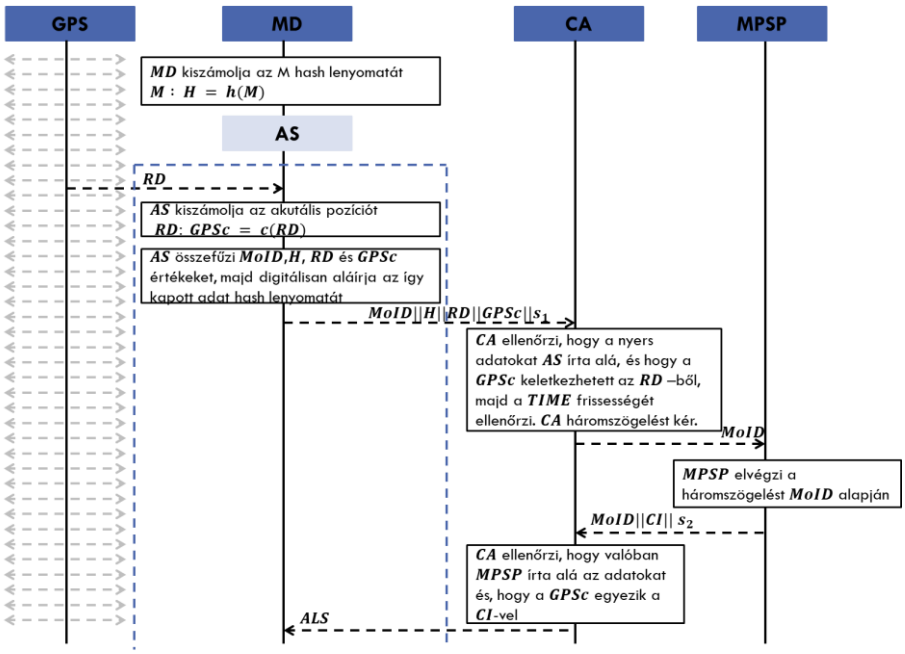


Ábra 1. A GPS biztonsági hiányosságai kriptográfiai szempontból

2.1.2. SZOFTVER SZINTRE INTEGRÁLT „HELYSZÍN-BÉLYEGZŐ" PROTOKOLL TERVEZÉSE ÉS MEGVALÓSÍTÁSA

A 2.1.1 fejezetben elmondottak szerint, vizsgálataim kezdetén nem állt rendelkezésre olyan eljárás, amely egyrészt a GPS jel szerkezetének változtatása nélkül képes biztosítani azon biztonsági kritériumokat, melyek a GPS műholdak és a GPS vevők közötti biztonságos csatorna kiépítéséhez szükségesek, másrészt garantálja a vevők által vett és számított adatok kriptográfiai védelmét. Az általunk 2013-ben készített, szoftver szintre integrált „helyszín-bélyegző" protokoll (lásd [2]) a második problémára nyújt megoldást. **A szoftver szintre integrált „Helyszín-bélyegző" protokoll egy olyan szoftver, amely egy megbízható harmadik fél és egy mobilszolgáltató segítségével garantálja a vevő által kezelt adatok kriptográfiai védelmét, emellett geodéziai hitelességet is biztosít bármely beépített GPS vevővel rendelkező eszköz számára.** A megoldás hardverfüggetlen, mivel a hitelesítést egy a vevőre telepített szoftverrel valósítjuk meg. A módszer alkalmazása során a koordináták számítása és aláírása a mobileszköz szoftver szintjén történik. A hiteles „Helyszín-bélyeghez" szükséges egy, a GPS rendszertől független rendszer helyadatainak összehasonlítása az eredetivel. Az eljárás során használt digitális

aláírás hitelesíti, hogy a számított GPS koordinátákat a vevőkészülék küldte a hitelesítő szervezetnek, és annak tartalma az átvitel során nem változott. A mobilszolgáltató által nyújtott helyinformációk összevetése a vevőkészülék által aláírt GPS koordinátákkal a helyadatok geodézia hitelességét hivatott igazolni, valamint megnöveli a kriptográfiai hitelesség szintjét is. A számított GPS koordináták frissességét a protokoll egy véletlen értékkel és a GPS navigációs üzenetéből nyert időinformációval biztosítja.

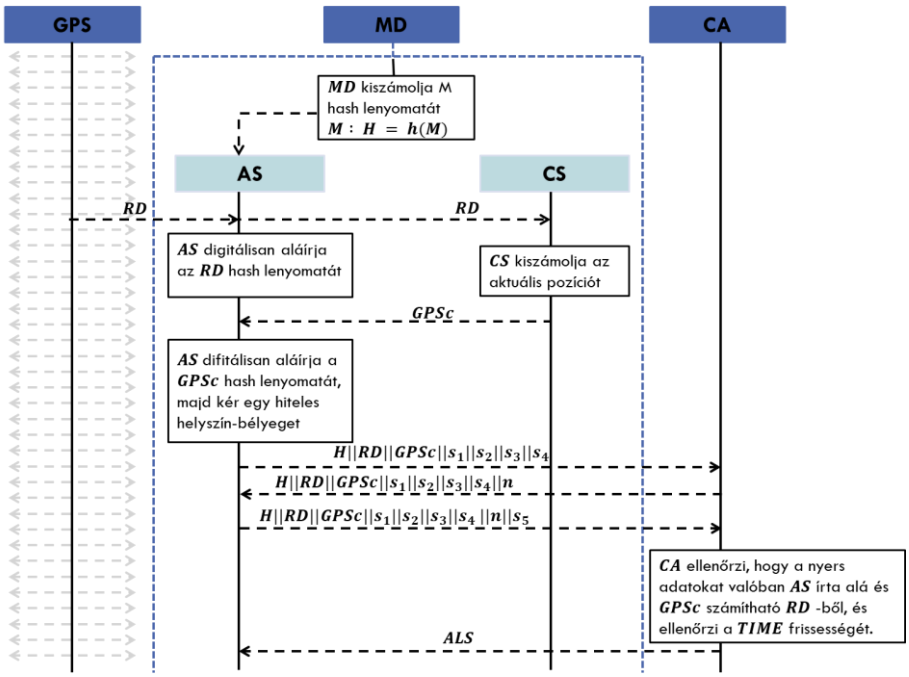


Ábra 2. Szoftver szintre integrált „Helyszín-bélyegző” protokoll

2.1.3. HARDVER SZINTRE INTEGRÁLT „HELYSZÍN-BÉLYEGZŐ” PROTOKOLL TERVEZÉSE ÉS MEGVALÓSÍTÁSA

Az általunk tervezett és kivitelezett második protokoll (lásd [2]), magasabb szintű kriptográfiai védelmet biztosít, mint az első, de ennek érdekében a vevőkészülékekben hardver szintű módosításokat kíván. A dolgozat 3.2.3.2. fejezetében részletesen ismertetett protokoll résztvevői a GPS rendszer, a vevőkészülék és egy megbízható harmadik fél, jelen esetben egy hitelesítő szervezet. **Elsődleges cél a folyamatban a műholdaktól érkező navigációs üzenet vétele és rögzítése úgy, hogy a vevőkészülékben a rosszindulatú módosítások ne történhessenek meg.** A módszer megvalósítása során a koordináták számítása és aláírása a mobileszköz hardver szintjére integrált. A protokoll esetében a digitális aláírás, valamint a biztonságos hardverelem hitelesíti, hogy az adott mobileszköz

fogadta az aláírt adatokat a műholdtól, továbbá ez az eszköz számította a GPS koordinátákat is. A számított GPS koordináták sértetlenségét is a digitális aláírás garantálja. A számított GPS koordináták frissességét a protokoll egy véletlen értékkel és a GPS navigációs üzenetéből nyert időinformációval biztosítja. A protokoll egy, a Debreceni Egyetem által *"Portable electronic device, system, and method for authenticating a document associated with a geographical location"* (lásd [3]) névvel szabadalmaztatott eljárás alapját képezi. Ezen módszer esetében a ProVerif automatikus helyesség bizonyító szoftver alkalmazásával igazoltam a protokoll által szolgáltatott biztonsági paraméterek közül kettőt.(lásd [7]



Ábra 3. Hardver szintre integrált „Helyszín-bélyegző" protokoll

2.2 MÁSODIK TÉZISPONT

A disszertációm negyedik fejezete a Modbus RTU ipari kommunikációs protokollt használó SCADA rendszerekkel kapcsolatos kutatási eredményeimet tartalmazza. Egy átfogó irodalomkutatás és feldolgozás során feltártam a Modbus RTU protokoll biztonsági hiányosságait, és az azok kiküszöbölésére már meglévő eljárásokat áttekintettem és elemeztem. Ebben a fejezetben ismertetem a kriptográfiailag biztonságos átviteli csatorna megvalósítására kidolgozott "Biztonságos Modbus RTU" protokollt is. **Az általam elkészített protokoll a Modbus RTU adatátviteli keretének és fizikai struktúrájának változtatása nélkül képes biztosítani a hiányzó**

alapvető biztonsági kritériumokat. A dolgozat második tézispontja a Modbus RTU protokoll hiányosságainak az "Attack-tree" módszerrel történő megvalósítását és a "Biztonságos Modbus RTU" protokoll tervezését, implementálását és tesztelését tartalmazza.

2.2.1. A MODBUS RTU HIÁNYOSSÁGAINAK FELTÁRÁSA

Meginni egy pohár tiszta vizet, felkapcsolni a villanyt, felhívni a családunkat, vagy igénybe venni valamilyen orvosi kezelést mind hétköznapi tevékenységek, melyek biztosításáért ún. kritikus infrastruktúrák felelősek. A kritikus infrastruktúrákhoz tartoznak a vízelosztó-, az áramszolgáltató és a telekommunikációs hálózatok, de az egészségügyi ellátórendszer létesítményei is. Az említett rendszerek esetében általában az irányítást, az adatgyűjtést és a rendszerek felügyelete SCADA rendszerek segítségével valósul meg. A SCADA rendszerek működése különböző kommunikációs protokollokra és számtalan terepi eszközre támaszkodik. Azonban a vezetéknélküli kommunikáció térnyerése, valamint a SCADA hálózatok online jellege miatt, a kritikus infrastruktúrák sebezhetősége jelentősen megnőtt az elmúlt évtizedekben. A fenti rendszereket nap, mint nap érik kiber támadások, melyek következményei nem csupán pénzügyi veszteség, vagy megromlott vállalati hírnév lehetnek, hanem az állampolgárok életének veszélyeztetése is. A nagy hálózatok gyakran régi, elavult kommunikációs protokollokra épülnek, mint a Modbus RTU ipari kommunikációs protokoll, de a teljes felújítás sokszor nem kivitelezhető, vagy csak nagyon magas költség mellett. A dolgozatom fókuszában a Modbus RTU ipari kommunikációs protokoll áll, amely a Modbus családdal együtt 1979 óta szabvány. A Modbus protokoll tervezése során a biztonságos kommunikáció, mint tervezési cél kimaradt, a megbízható működésre és a megfelelő sebességre fektettek csak hangsúlyt. A dolgozatom 4.2.1. és 4.2.2. fejezetében bemutatott kutatásaim célja a Modbus RTU alapú SCADA rendszerek sebezhetőségének vizsgálata a kapcsolódó szakirodalom átfogó áttekintésével és elemzésével, továbbá az „Attack-Tree” módszer alkalmazásával. (lásd [4], [5], [6]). **A kutatás eredményeként megtalált biztonsági hiányosságok egyrészről a résztvevők hitelesítésének, valamint az üzenetek bizalmasságának, integritásának és frissességének hiánya az adatátvitelre használt csatornán, másrészről a protokoll érzékenysége a MITM (Man in the Middle) és a DoS (Denial of Service) típusú támadásokra. Harmadrészt, hogy fennáll a csatornán haladó üzenetek lehallgatásának, módosításának, fabrikálásának és az üzenettovábbítás megszakításának lehetősége. A vonatkozó szakirodalomban, a vizsgálataim kezdetén, a fenti problémákra nem volt létező megoldás.**

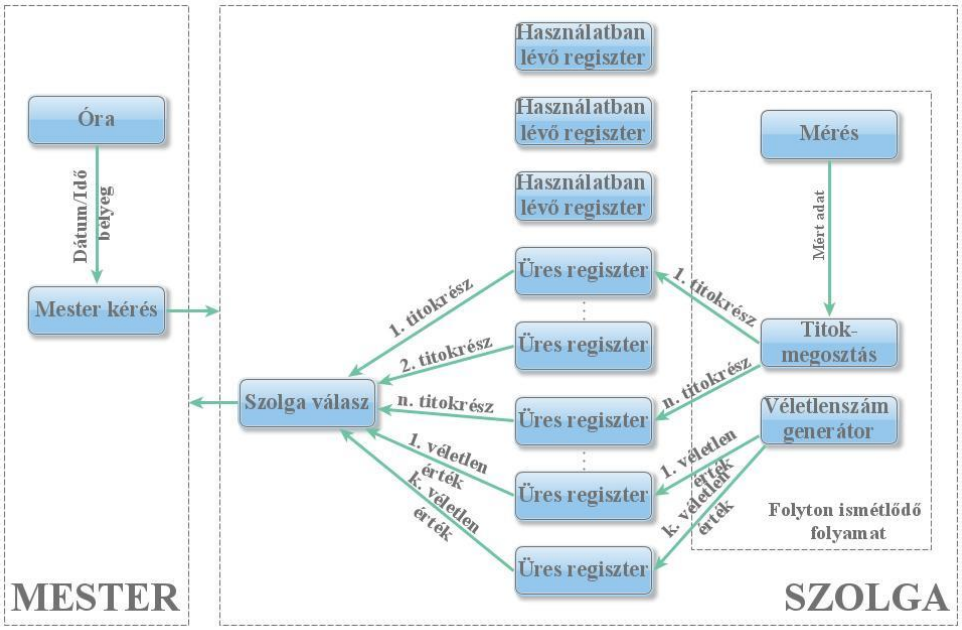
2.2.2. BIZTONSÁGOS MODBUS RTU KOMMUNIKÁCIÓ TERVEZÉSE ÉS MEGVALÓSÍTÁSA

A dolgozat 4.2.3-as fejezetében a Modbus RTU ipari kommunikációs protokoll biztonsági hiányosságainak megoldására kifejlesztett “Biztonságos Modbus RTU” protokollt mutatom be. A javasolt módszer azon alapul, hogy a Modbus RTU

protokoll az adatátvitel során nem használja ki maximálisan a lehetséges üzenethosszt, és az üzenetváltás gyakorisága relatíve alacsony. Jellemzően a gyakorlatban a SCADA rendszerekben mind az MTU (Master Terminal Unit), mind a terepi eszközök rendelkeznek egy beépített AES (Advanced Encryption Standard) titkosítóval, mely a szabványos kéréseket és válaszokat képes titkosítani a csatornán. Ez az ún. AES motor az eszközök sajátja, egy a gyártók által beépített szolgáltatás, mely független az alkalmazott ipari kommunikációs protokolltól. Meg kell jegyezni, hogy habár a beépített AES titkosító elősegíti a biztonságos átviteli csatorna kiépítését, de önmagában nem oldja meg a fentebb bemutatott biztonsági hiányosságokat.

Az általunk tervezett és megvalósított megoldás a résztvevők hitelesítését, az üzenetek adatintegritását, frissességét és bizalmasságát garantálja. A közös titkos kulcs és a kihívás értékek hitelesítik a Mestert a Szolga felé és fordítva. Az üzenetek bizalmassága egy beépített AES titkosítóval biztosított. Az adatok integritását a Szenzor típusú Szolgák esetén egy ún. „összekeverés" nevű eljárás biztosítja, amely titokmegosztáson alapul. (lásd [8])

A „Biztonságos Modbus RTU" protokoll gyakorlati alkalmazhatóságának ellenőrzésére a Debreceni Egyetem Műszaki Karának Villamosmérnöki és Mechatronikai Tanszékén megterveztünk és kiviteleztünk egy teszt rendszert Az alábbiakat tapasztaltuk: Egy egyszeri üzenetváltás sebessége ötször nagyobb a javasolt biztonságos módszer alkalmazása esetén, mint az eredeti protokoll használatával. A terepi eszközök teljesítménye nem csökkent, minden funkciójuk hibátlanul, a megszokott módon működött. A szolga oldalon történő válasz üzenet generálásának ideje 400%-kal nőtt, ebbe a kommunikáció inicializáló lépései nem kerültek beszámításba. A mester felé történő üzenettovábbításhoz szükséges idő hossza 23%-kal nőtt. A tesztelési periódus során az elutasított üzenetek aránya 1:15000 volt. A teszt alapján kijelenthetjük, hogy a módszer kis számítási kapacitással rendelkező terepi eszközök esetén is alkalmazható.



Ábra 4. Szenzor tipusú szolga kommunikáció “Biztonságos Modbus RTU” esetén

DEBRECENI EGYETEM

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

Nyilvántartási szám: DEENK/182/2020.PL
Tárgy: PhD Publikációs Lista

Jelölt: Csernusné Ádámkó Éva
Neptun kód: TL4X9T
Doktori Iskola: Informatikai Tudományok Doktori Iskola
MTMT azonosító: 10039859

A PhD értekezés alapjául szolgáló közlemények

Magyar nyelvű tudományos közlemények hazai folyóiratban (1)

1. Jakabóczki, G., Szemes, P. T., **Csernusné Ádámkó, É.**: A MODBUS RTU protokoll biztonságtechnikai vizsgálata, új kriptográfiai megoldások tesztelése = Security evaluation of MODBUS RTU protocol, testing new cryptographic methods.
   Int. J. Eng. Manag. Sci. 1 (2), 35-42, 2016. EISSN: 2498-700X.
   DOI: http://dx.doi.org/10.21791/IJEMS.2016.2.5.

Idegen nyelvű tudományos közlemények hazai folyóiratban (1)

2. **Csernusné Ádámkó, É.**: Security analysis of a "Location-stamping" protocol for GPS coordinates.
   Int. J. Eng. Manag. Sci. 2 (2), 1-12, 2017. EISSN: 2498-700X.
   DOI: http://dx.doi.org/10.21791/IJEMS.2017.2.1.

Idegen nyelvű tudományos közlemények külföldi folyóiratban (4)

3. **Csernusné Ádámkó, É.**, Jakabóczki, G., Szemes, P. T.: Proposal of a Secure Modbus RTU communication with Adi Shamir's secret sharing method.
   Int. J. Elect. Telecomm. 64 (2), 107-114, 2018. ISSN: 2081-8491.
   DOI: http://dx.doi.org/10.24425/119357

4. **Csernusné Ádámkó, É.**, Jakabóczki, G.: Vulnerabilities of MODBUS rtu protocol?: a case study.
   Anale. Univ. Oradea. Fasc. Manag. Techn. Engin. 24 (1), 203-206, 2015. ISSN: 1583-0691.

5. **Csernusné Ádámkó, É.**, Szemes, P. T., Niitsuma, M.: Investigation on the heating system of the Mechatronics Research Center building using OLAP technology.
   Environ. Eng. Manag. J. 13 (11), 2733-2742, 2014. ISSN: 1582-9596.
   IF: 1.065

6. **Csernusné Ádámkó, É.**, Pethő, A.: Location-stamp for GPS coordinates.
   Acta Univ. Sap., Inf. 5 (1), 63-76, 2013. ISSN: 1844-6086.

Magyar nyelvű konferencia közlemények (1)

7. **Csernusné Ádámkó, É.**, Pethő, A.: "Helyszín-bélyegzés", hitelesített GPS koordináták.
In: Az elmélet és gyakorlat találkozása a térinformatikában II. : Térinformatikai Konferencia és Szakkiállítás Debrecen 2011. Szerk.: Lóki József, Debreceni Egyetem, Debrecen, 381-387, 2011. ISBN: 9789633181164

Idegen nyelvű konferencia közlemények (1)

8. **Csernusné Ádámkó, É.**, Jakabóczki, G.: Security analysis of Modbus RTU.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Szerk.: Kocsis Imre, University of Debrecen Faculty of Engineering, Debrecen, 5-11, 2015. ISBN: 9789634739166

Szabadalmak (1)

Bérczes, A., **Csernusné Ádámkó, É.**, Folláth, J., Pethő, A.: Portable electronic device, system and method for authenticating a document associated with a geographical location. 2013
Hatáskör: USA
Bejelentés ideje: 2012.11.09
Szabadalmi szám: US20130117572 A1

További közlemények

Magyar nyelvű könyvrészletek (1)

9. Bánóczy, E., **Csernusné Ádámkó, É.**, Husi, G., Piros, S., Szász, C., Szemes, P. T., Vitéz, A. C.: Épületmechatronika.
In: Fenntartható energetika megújuló energiaforrások optimalizált integrálásával. Szerk.: Kalmár Ferenc, Akadémiai Kiadó, Budapest, 119-166, 2014. ISBN: 9789630595407

Idegen nyelvű tudományos közlemények hazai folyóiratban (3)

10. **Csernusné Ádámkó, É.**: Online self-learning.
Int. J. Eng. Manag. Sci. 5 (1), 542-553, 2020. EISSN: 2498-700X.
DOI: http://dx.doi.org/10.21791/IJEMS.2020.1.44

11. **Csernusné Ádámkó, É.**: Gamification in programming: a short introductory session in programming with online games.
Int. J. Eng. Manag. Sci. 3 (5), 16-22, 2018. EISSN: 2498-700X.
DOI: http://dx.doi.org/10.21791/IJEMS.2018.5.2.

DEBRECENI EGYETEM
DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

12. **Csernusné Ádámkó, É.**, Szemes, P. T.: Evaluation of Consumer Behavior in the Building mechatronics research centre.
Recent Innovat. Mechatron. 1 (1-2), 1-5, 2014. EISSN: 2064-9622.

Magyar nyelvű konferencia közlemények (2)

13. **Csernusné Ádámkó, É.**: Játék alapú kódolás a középiskolában.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Imre Kocsis, Institute of English and American Studies, University of Debrecen, Debrecen, 5-10, 2017. ISBN: 9789634739814
14. **Csernusné Ádámkó, É.**, Szemes, P. T.: Az épületmechatronikai kutatóközpont szerepe a debreceni épületmechatronikai képzésben.
In: VIII. Energetikai konferencia 2013: 'Az energetika oktatása'. Szerk.: Szakál Anikó, Óbudai Egyetem, Budapest, 35-40, 2013. ISBN: 9786155018923

Idegen nyelvű konferencia közlemények (3)

15. **Csernusné Ádámkó, É.**: Online Self-Learning Methods for Programming.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Kocsis Imre, University of Debrecen Faculty of Engineering, Debrecen, 4-7, 2020. ISBN: 9789634901747
16. **Csernusné Ádámkó, É.**: Comparative analysis of project-based programming courses in Hungarian and foreign classes.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Imre Kocsis, University of Debrecen Faculty of Engineering, Debrecen, 5-12, 2016. ISBN: 9789634739456
17. **Csernusné Ádámkó, É.**: Design and Correctness Proof of Cryptographic Protocols.
In: Proceedings of the Conference on Problem-based Learning in Engineering Education. Ed.: Kocsis Imre, University of Debrecen Faculty of Engineering, Debrecen, 4-9, 2014. ISBN: 9789634737612

A közlő folyóiratok összesített impakt faktora: 1,065
A közlő folyóiratok összesített impakt faktora (az értekezés alapjául szolgáló közleményekre): 1,065

DEBRECENI EGYETEM Egyetemi és Nemzeti Könyvtár

A DEENK a Jelölt által az iDEa Tudóstérbe feltöltött adatok bibliográfiai és tudománymetriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2020.06.10.

3 LIST OF PAPERS RELATED TO THE THESIS WITH CITATIONS RELEVÁNS PUBLIKÁCIÓS LISTA IDÉZÉSEKKEL

[1] **Csernusné Ádámkó Éva**, Pethő Attila “Helyszín bélyegzés”, hitelesített GPS koordináták In: Lóki, J (szerk.) Az elmélet és gyakorlat találkozása a térinformatikában II. : II. Térinformatikai Konferencia és Szakkiállítás Debrecen Debrecen, Magyarország : DE TTK Földrajzi Tanszékcsoport, (**2011**) pp. 381-387. , 7 p.

[2] **Ádámkó**, **E**., & Pethő, A. (**2013**). Location-stamp for GPS coordinates. Acta Universitatis Sapientiae, Informatica, 5(1), 63-76.

[3] Bérczes, A., **ÁDÁMKÓ, É. C.**, Folláth, J., & Pethõ, A. (**2013**). U.S. Patent Application No. 13/673,085.

- Freeze-Skret, J. (2016). U.S. Patent No. 9,432,390. Washington, DC: U.S. Patent and Trademark Office.
- Kostiainen, K. (2017). U.S. Patent No. 9,787,667. Washington, DC: U.S. Patent and Trademark Office.
- Cohen, R. H. (2017). U.S. Patent No. 9,800,415. Washington, DC: U.S. Patent and Trademark Office.
- Jones, R. K., Steger, C., Brachet, N., Alizadeh-Shabdiz, F., Broadstone, A., & Morrin, J. (2017). U.S. Patent No. 9,817,101. Washington, DC: U.S. Patent and Trademark Office.
- Salmela, P., & Fornehed, J. (2018). U.S. Patent Application No. 15/551,683.

[4] **Ádámkó Éva**, Jakabóczki Gábor Security analysis of Modbus RTU pp. 5-11. In: Kocsis, Imre (szerk.) Proceedings of the Conference on Problem-based Learning in Engineering Education Debrecen, Magyarország: University of Debrecen Faculty of Engineering, (**2015**) p. 98

[5] Jakaboczki, G., & **Adamko, E.** (**2015**). Vulnerabilities Of Modbus RTU Protocol–A Case Study. Annals Of The Oradea University, Fascicle Of Management And Technological Engineering, (1).

- Muñoz, N., & Davensor, C. (2016). Explotando vulnerabilidades en el protocolo MODBUS TCP/IP.

- Dogaru, D. I., & Dumitrache, I. (2017, May). Robustness of Power Systems in the Context of Cyber Attacks. In 2017 21st International Conference on Control Systems and Computer Science (CSCS) (pp. 506-512). IEEE.
- Tranca, D. C., Banu, C. I., & Rosner, D. (2018). EGIFM--Extendable Gateway and Industrial Firewall for ModBus. eLearning & Software for Education, 4.
- Urdaneta Velasquez, M. (2018). Attaques informatiques sur le réseau de contrôle du trafic routier (Doctoral dissertation, École Polytechnique de Montréal).
- Velasquez, M. U. (2018). Attaques Informatiques sur le Réseau de Contrôle du Trafic Routier (Doctoral dissertation, Ecole Polytechnique, Montreal (Canada)).

[6] Jakabóczki G, Szemes P T, **Ádámkó É** A MODBUS RTU protokoll biztonságtechnikai vizsgálata, új kriptográfiai megoldások tesztelése = Security evaluation of MODBUS RTU protocol, testing new cryptographic methods INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES / MŰSZAKI ÉS MENEDZSMENT TUDOMÁNYI KÖZLEMÉNYEK 1: 2 pp. 35-42. , 8 p. (**2016**)

[7] **Ádámkó, É.** (**2017**). Security analysis of a „Location-stamping" protocol for GPS coordinates. Műszaki és Menedzsment Tudományi Közlemények, 2(2), 1-12.

[8] **Ádámkó, É.**, Jakabóczki, G., & Szemes, P. T. (**2018**). Proposal of a Secure Modbus RTU communication with Adi Shamir's secret sharing method. International Journal of Electronics and Telecommunications, 64(2), 107-114.

- Chromik, J. J., Remke, A., & Haverkort, B. R. (2018). An integrated testbed for locally monitoring SCADA systems in smart grids. Energy Informatics, 1(1), 56.
- Volkova, A., Niedermeier, M., Basmadjian, R., & de Meer, H. (2018). Security challenges in control network protocols: A survey. IEEE Communications Surveys & Tutorials, 21(1), 619-639.
- Tidrea, A., Korodi, A., & Silea, I. (2019). Cryptographic Considerations for Automation and SCADA Systems Using Trusted Platform Modules. Sensors, 19(19), 4191

- Gamess, E., Smith, B., & III, G. F. PERFORMANCE EVALUATION OF MODBUS TCP IN NORMAL OPERATION AND UNDER ADistributed DENIAL OF SERVICE ATTACK. International Journal of Computer Networks and Communications 12(2):1-21 (2020)