electronics

Editorial

In-Vehicle Networking/Autonomous Vehicle Security for Internet of Things/Vehicles

Taeshik Shon

Department of Software and Computer Engineering, Ajou University, Suwon 16499, Korea; tsshon@ajou.ac.kr

Citation: Shon, T. In-Vehicle Networking/Autonomous Vehicle Security for Internet of Things/Vehicles. *Electronics* **2021**, *10*, 637. https://doi.org/10.3390/electronics10060637

Received: 3 March 2021
Accepted: 5 March 2021
Published: 10 March 2021

1. Introduction

In recent years, vehicles have become one of the most common examples in the area of ICT convergence applications and services. In simple terms, this means that a vehicle system is composed of various internet and communication technologies such as in-vehicle networking, wireless communications such as 4G/LTE, 5G, 802.11x, and Bluetooth that enables Internet access, including cloud and V2X communications (Vehicle to Everything) such as Vehicle to Vehicle (V2V), Vehicle to Pedestrian (V2P), Vehicle to Devices (V2D), Vehicle to Grid (V2G), and Vehicle to Infrastructure (V2I). In addition, in-vehicle system performance and user-provided services are ever-advancing by adopting artificial intelligence technologies with deep learning methods [1,2]. They offer a variety of improved features that allow vehicles to inter-work with the outside world based on high-speed and high-capacity internet technology being accelerated by 5G. At the same time, potential cybersecurity threats on vehicle systems and networks are rapidly growing, such as user privacy and payment information disclosure, unauthorized vehicle software updates, stealing smart keys/passwords, vehicle communication protocol forgery and injection, DoS/DDoS, physical jamming, etc. In order to provide more secure and reliable services for vehicles, both security and safety should be carefully considered [3–8].

The objective of this Special Issue is to focus on the technical contribution, analysis, design, performance simulation, and implementation of in-vehicle networking, autonomous network security for the Internet of Things/vehicles, safety detection, safety, and security on the virtualized automotive platform. The topics of interest include Automotive networking, In-vehicle network security, Autonomous vehicle security, V2X applications and services for security, Internet of Things/Vehicles, Industrial Internet of Things for vehicle security, Safety detection and fault management, Security and safety on an automotive virtualized platform, Performance and fault simulation, and Platform virtualization.

2. In-Vehicle Networking/Autonomous Vehicle Security Researches

In "A Reactive and On-Chip Sensor Circuit for NBTI (Negative Bias Temperature Instability) and PBTI (Positive Bias Temperature Instability) Resilient SRAM (Static Random-Access Memory) Design" [9], Nandakishor Yadav et al. take on the issue of Sensor Circuit for NBTI and PBTI Resilient SRAM Design for an autonomous vehicle. Process Variation (PV), Bias Temperature Instability (BTI), and Time-Dependent Dielectric Breakdown (TDDB) are critical factors that affect the reliability of semiconductor chip design. They cause the system to be unstable and increase the soft error rate. In this paper, a compact on-chip degradation technique using runtime leakage current monitoring has been proposed. The proposed sensor-based adaptive technique compensates for the variation due to PV and aging using the body-bias-voltage-generator circuit. Simulation experiments for 3- and 10-year stress have been performed. Simulation results proved the superiority of the proposed sensor, which provides 33% (up to 0.75 V) more output voltage and 98% sensitivity at a 1 V supply voltage compared to the state-of-the-art sensor. The proposed technique mitigates up to 80% PV and BTI effects in SRAM compared to the state-of-the-art techniques.

Nandakishor Yadav et al. [10] addressed the issue of Design of a Voltage to Time Converter with High Conversion Gain for Reliable and Secure Autonomous Vehicles. The automation of vehicles requires a secure, reliable, and real-time on-chip system. These systems also require very high-speed and compact on-chip Analog to Digital Converters (ADC). The conventional ADC cannot fulfill this requirement. In this paper, we proposed a Darlington pair and source biasing-based high speed, secure, and reliable Voltage to Time Converter (VTC). It is a compact, high-speed design and gives a high conversion gain. The source biasing also helps increase the input voltage range. The conversion gain of the proposed circuit is 101.43 ns/v, which is 52 times greater than the gain achieved by the state-of-the-art design. It also shows less effect of process variation and bias temperature instability.

The article "Optimized Node Clustering in VANETs by Using Meta-Heuristic Algorithms" by Waleed Ahsan et al. [11], discusses optimized node clustering issues in VANETs. In a Vehicular Ad-Hoc Network (VANET), the vehicles are the nodes, and these nodes communicate with each other. On the road, vehicles are continuously in motion causing a dynamic change in the network topology. It is more challenging when there is a higher node density. These conditions create many difficulties for network scalability and optimal route-finding in VANETs. Clustering protocols are being used frequently to solve such types of problems. In this paper, we proposed the Grasshoppers' Optimization-based (GOA) node clustering algorithm for VANETs for optimal cluster head selection. The proposed algorithm reduced the network overhead in unpredictable node density scenarios. To do so, different experiments were performed for the comparative analysis of GOA with other state-of-the-art techniques such as dragonfly algorithm, Grey Wolf Optimizer (GWO), and Ant Colony Optimization (ACO). Plentiful parameters, such as the number of clusters, network area, node density, and transmission range, were used in various experiments. The outcome of these results indicated that GOA outperformed the existing methodologies. Lastly, the application of GOA in the Flying Ad-Hoc Network (FANET) domain was also proposed for next-generation networks.

In "Design and Development of BTI Model and 3D InGaAs HEMT-Based SRAM for Reliable and Secure Internet of Things Application" [12], Nandakishor Yadav et al. take on the issue of the BTI model and 3D InGaAs HEMT-based SRAM for vehicle applications. It is broadly accepted that the silicon-based CMOS has touched its scaling limits and alternative substrate materials are needed for future technology nodes. An Indium-Gallium-Arsenide (InGaAs)-based device is well situated for further technology nodes. This material also has better mobility of the electrons and holes for the high performance and real-time system design. The improved mobility helps increase the operating frequency of the device, which is useful for Internet of Things (IoT) applications. However, InGaAs -based High Electron Mobility Transistors (HEMT) limit the reliability of the device due to the presence of dangling bonds at the channel–gate insulator interfaces. Weak dangling-bonds get broken under electric stress, and positive hydrogen atoms are trapped into the oxide. This charge trapping depends on the material parameters and device geometry. In this paper, the existing Bias-Temperature-Instability (BTI) model is modified based on the material parameters and device geometry. Charge trapping and annealing constants are the most critical BTI model parameters, which are modeled and evaluated based on different HEMT material parameters. The proposed model was compared to experimental and TCAD simulation results. The proposed model has been used for the lifetime prediction of the InGaAs HEMT-based Static Random-Access Memory (SRAM) cell since it is used to store and process the information in the IoT applications.

In "Low-Power RTL Code Generation for Advanced CNN Algorithms toward Object Detection in Autonomous Vehicles" [13], Youngbae Kim et al. take on the issue of low power RTL code generation for an autonomous vehicle. In the implementation process of a Convolution Neural Network (CNN)-based object detection system, the primary issues are power dissipation and limited throughput. Even though we utilize ultra-low power dissipation devices, the dynamic power dissipation issue will be difficult to resolve. During the operation of the CNN algorithm, there are several factors such as the heating problem generated from the massive computational complexity, the bottleneck generated in data transformation and by the limited bandwidth, and the power dissipation generated from redundant data access. This article proposed the low-power techniques, applied them to the CNN accelerator on the FPGA and ASIC design flows, and evaluated them on the Xilinx ZCU-102 FPGA SoC hardware platform and 45 nm technology for ASIC, respectively. Our proposed low-power techniques are applied at the Register-Transfer-Level (RT-level), targeting FPGA and ASIC. In this article, we achieved up to a 53.21% power reduction in the ASIC implementation and saved 32.72% of the dynamic power dissipation in the FPGA implementation. This showed that our RTL low-power schemes have a powerful possibility of dynamic power reduction when applied to the FPGA and ASIC design flows for the implementation of the CNN-based object detection system.

The article "Sensitive, Linear, Robust Current-To-Time Converter Circuit for Vehicle Automation Application" [14] by Nandakishor Yadav et al., discusses the robust current-to-time converter circuit for vehicle automation. Voltage-to-time and current-to-time converters have been used in many recent works as a voltage-to-digital converter for artificial intelligence applications. In general, most of the previous designs use the current-starved technique or a capacitor-based delay unit, which is non-linear, expensive, and requires a large area. In this paper, we proposed a highly linear current-to-digital converter. An optimization method is also proposed to generate the optimal converter design containing the smallest number of PMOS and sensitive circuits such as a differential amplifier. This enabled our design to be more stable and robust toward Negative Bias Temperature Instability (NBTI) and process variation. The proposed converter circuit implements the point-wise conversion from current-to-time, and it can be used directly for a variety of applications, such as Analog-to-Digital Converters (ADC), used in built-in Computational Random Access (C-RAM) memory. The conversion gain of the proposed circuit is 3.86 ms/A, which is 52 times greater than the conversion gains of state-of-the-art designs. Further, various Time-to-Digital Converter (TDC) circuits are reviewed for the proposed current-to-time converter, and we recommend one circuit for a complete ADC design.

In "An Anonymous Device to Device Authentication Protocol Using ECC and Self Certified Public Keys Usable in Internet of Things Based Autonomous Devices" [15], Bander A. Alzahrani et al. take on the issue of device authentication protocol for the Internet of Things based on autonomous devices. Two party authentication schemes can be good candidates for deployment in Internet of Things (IoT)-based systems, especially in systems involving fast moving vehicles. The Internet of Vehicles (IoV) requires fast and secure device-to-device communication without interference of any third party during the communication, and this task can be carried out after the registration of vehicles with a trusted certificate issuing party. Recently, several authentication protocols were proposed to enable a key agreement in two party settings. In this study, we analyzed two recent protocols and showed that both protocols are insecure against the Key Compromise Impersonation Attack (KCIA) and lack user anonymity. Therefore, this paper proposed an improved protocol that does not only resist the KCIA and related attacks, but also offered comparable computation and communication. The security of the proposed protocol is tested under a formal model, as well as using well known Burrows–Abadi–Needham (BAN) logic along with a discussion on security features. While resisting the KCIA and related attacks, the proposed protocol also provides a comparable trade-off between security features and efficiency and completes a round of key agreement in just 13.42 ms, which makes it a promising candidate to be deployed in IoT environments.

In "Packet Preprocessing in CNN-Based Network Intrusion Detection System" [16], Wooyeon Jo et al. take on the issue of the CNN-based network intrusion detection system. The proliferation of various connected platforms, including the Internet of Things, Industrial Control Systems (ICSs), connected cars, and in-vehicle networks, has resulted in the simultaneous use of multiple protocols and devices. Chaotic situations caused by the usage of different protocols and various types of devices, such as heterogeneous networks, implemented differently by vendors renders the adoption of a flexible security solution difficult, such as recent deep learning-based Intrusion Detection System (IDS) studies. These studies optimized the deep learning model for their environment to improve performance, but the basic principle of the deep learning model used was not changed. Therefore, this can be called a next-generation IDS with a model that has little or no requirements. Some studies proposed IDS based on the unsupervised learning technology that does not require labeled data. However, not using the available assets, such as network packet data, is a waste of resources. If the security solution considers the role and importance of the devices constituting the network and the security area of the protocol standard by experts, the assets can be well used, but it will no longer be flexible. Most deep learning model-based IDS studies used the Recurrent Neural Network (RNN), which is a supervised learning model, since the characteristics of the RNN model, especially when the Long-Short Term Memory (LSTM) is incorporated, are better configured to reflect the flow of the packet data stream over time, and thus perform better than other supervised learning models such as the Convolutional Neural Network (CNN). However, if the input data induce the CNNs kernel to sufficiently reflect the network characteristics through proper preprocessing, it could perform better than other deep learning models in the IDS network. Hence, we proposed the first preprocessing method, called "direct", for the IDS network that can use the characteristics of the kernel using the minimum protocol information, field size, and offset. In addition to direct, we proposed two more preprocessing techniques called "weighted" and "compressed". Each requires additional network information, therefore, direct conversion was compared with the related studies. Including direct, the proposed preprocessing methods are based on field-to-pixel philosophy, which can reflect the advantages of CNN by extracting the convolutional features of each pixel. Direct is the most intuitive method of applying field-to-pixel conversion to reflect an image's convolutional characteristics in the CNN. Weighted and compressed are conversion methods used to evaluate the direct method. Consequently, the IDS constructed using a CNN with the proposed direct preprocessing method demonstrating a meaningful performance in the NSL-KDD dataset.

3. Conclusions

We would like to take this opportunity to thank all the authors for submitting papers to this Special Issue. We also hope that the readers will find new and useful information on In-Vehicle Networking/Autonomous Vehicle Security for Internet of Things/Vehicles and the related cybersecurity technology.

Funding: This research received no external funding.

Acknowledgments: We would like to thank all the researchers who submitted articles to this special issue. We are also grateful to all the reviewers who helped in the evaluation of the manuscripts and made very valuable suggestions to improve the quality of contributions. We would like to acknowledge the editorial board of Electronics, who invited us to guest edit this special issue. We are also grateful to the Electronics Editorial Office staff who worked thoroughly to maintain the rigorous peer-review schedule and timely publication.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kim, S.; Jo, W.; Shon, T. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. *Appl. Soft Comput.* **2020**, *88*, 106017. [CrossRef]
2. Kwon, S.; Yoo, H.; Shon, T. IEEE 1815.1-Based Power System Security with Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System. *IEEE Access* **2020**, *8*, 77572–77586. [CrossRef]
3. Mahmood, K.; Chaudhry, S.A.; Naqvi, H.; Shon, T.; Farooq Ahmad, H. A lightweight message authentication scheme for Smart Grid communications in power sector. *Comput. Electr. Eng.* **2016**, *52*, 114–124. [CrossRef]
4. Yoo, H.; Shon, T. Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. *Future Gener. Comput. Syst.* **2016**, *61*, 128–136. [CrossRef]

5. Chaudhry, S.A.; Shon, T.; Al-Turjman, F.; Alsharif, M.H. Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. *Comput. Commun.* **2020**, *153*, 527–537. [CrossRef]
6. Jo, W.; Shin, Y.; Kim, H.; Yoo, D.; Kim, D.; Kang, C.; Jin, J.; Oh, J.; Na, B.; Shon, T. Digital Forensic Practices and Methodologies for AI Speaker Ecosystems. *Digit. Investig.* **2019**, *29*, S80–S93. [CrossRef]
7. Shin, Y.; Kim, H.; Kim, S.; Yoo, D.; Jo, W.; Shon, T. Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. *Forensic Sci. Int. Digit. Investig.* **2020**, *3*, 301010. [CrossRef]
8. Lee, S.; Jo, W.; Eo, S.; Shon, T. ExtSFR: Scalable file recovery framework based on an Ext file system. *Multimed. Tools Appl.* **2019**, *79*, 1–19. [CrossRef]
9. Yadav, N.; Kim, Y.; Alashi, M.; Choi, K. A Reactive and On-Chip Sensor Circuit for NBTI and PBTI Resilient SRAM Design. *Electronics* **2020**, *9*, 326. [CrossRef]
10. Yadav, N.; Kim, Y.; Alashi, M.; Ken Choi, K. Design of a Voltage to Time Converter with High Conversion Gain for Reliable and Secure Autonomous Vehicles. *Electronics* **2020**, *9*, 384. [CrossRef]
11. Ahsan, W.; Khan, M.; Aadil, F.; Maqsood, M.; Ashraf, S.; Nam, Y.; Rho, S. Optimized Node Clustering in VANETs by Using Meta-Heuristic Algorithms. *Electronics* **2020**, *9*, 394. [CrossRef]
12. Yadav, N.; Alashi, M.; Choi, K. Design and Development of BTI Model and 3D InGaAs HEMT-Based SRAM for Reliable and Secure Internet of Things Application. *Electronics* **2020**, *9*, 469. [CrossRef]
13. Kim, Y.; Kim, H.; Yadav, N.; Li, S.; Choi, K. Low-Power RTL Code Generation for Advanced CNN Algorithms toward Object Detection in Autonomous Vehicles. *Electronics* **2020**, *9*, 478. [CrossRef]
14. Yadav, N.; Kim, Y.; Alashi, M.; Choi, K. Sensitive, Linear, Robust Current-To-Time Converter Circuit for Vehicle Automation Application. *Electronics* **2020**, *9*, 490. [CrossRef]
15. Alzahrani, B.; Chaudhry, S.; Barnawi, A.; Al-Barakati, A.; Shon, T. An Anonymous Device to Device Authentication Protocol Using ECC and Self Certified Public Keys Usable in Internet of Things Based Autonomous Devices. *Electronics* **2020**, *9*, 520. [CrossRef]
16. Jo, W.; Kim, S.; Lee, C.; Shon, T. Packet Preprocessing in CNN-Based Network Intrusion Detection System. *Electronics* **2020**, *9*, 1151. [CrossRef]