Hindawi
Security and Communication Networks
Volume 2022, Article ID 9865621, 4 pages
https://doi.org/10.1155/2022/9865621

Editorial

Security Hardened and Privacy Preserved Vehicle-to-Everything (V2X) Communication

Azeem Irshad,[1] **Muhammad Shafiq**,[2] **Shehzad Ashraf Chaudhry**,[3] **and Muhammad Usman**[4]

[1]*Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad, Pakistan*
[2]*Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea*
[3]*Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*
[4]*Faculty of Computing Engineering and Science, University of South Wales, Pontypridd CF37 1DL, UK*

Correspondence should be addressed to Muhammad Shafiq; shafiq@ynu.ac.kr

Received 19 March 2022; Accepted 19 March 2022; Published 12 April 2022

Vehicle-to-everything (V2X) communications have recently gained concentration of researchers for both, academia as well as industry. In the V2X system, the information is communicated from vehicle sensors to other vehicles, infrastructure, pedestrians, and mobile network cloud through high-bandwidth reliable links [1–4]. The technology may greatly improve the driver's awareness of imminent hazards, thereby reducing the severity of accidents, fatalities, or possible collisions with other vehicles. The V2X technology brings efficiency through creating warning alerts for drivers, imparting the information of alternative routes for avoiding possible traffic congestions and pinpointing available parking spaces. Such critical situations might become problematic if the security and privacy of V2X communication system is compromised [5–8]. Thus, V2X vehicles along with efficiency, reliability, and safety parameters require more secure and robust communication protocols to meet the upcoming security challenges. Moreover, the wireless nature of the system might become challenging in affording secure and ubiquitous connectivity to the V2X network [9–13]. This is crucial to create a fail-safe infrastructure of modern traffic scenario regarding smart cities since security and privacy issues are quite prevalent in our daily lives.

This special issue encompasses 13 research articles focusing on security and privacy of vehicular networks. The details of these articles are summarized as follows.

The authors in a research article titled "Implementation of Blockchain Consensus Algorithm on Embedded Architecture" presented study of the feasibility as well as the gain realized by using an architecture adopted at Ethereum PoW on FPGAs [14]. The concept of finding optimized solutions adapted to the specific constraints of blockchain-based applications such as execution time, number of required nodes, and suitable data security algorithms are heavily researched in the literature. The paper also presents the implementation of an embedded-blockchain approach. This system presents a hybrid implementation of ethereum nodes on Raspberry Pi on one side and of PoW consensus on FPGA. This may prove to be a significant proposal for future implementations since it provides the possibility to set up an ASIC to accelerate the POW execution.

The authors in a research article titled "New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT" proposed new authentication scheme for health care systems cloud-IoT [15]. Before presenting the proposed work, the authors demonstrate the vulnerabilities and security issues of previous proposed studies including Sharma and Kalra's scheme. The authors discover few weaknesses in the Sharma and Kalra's protocol along with password guessing and smart card stolen attacks. The simulation tests as performed under Scyther tool confirm that the lightweight proposed protocol satisfies up-to-date security requirements. The formal and informal analysis also validates the findings of the obtained results in the performance evaluation.

The authors in a research article titled "Chaotic Reversible Watermarking Method Based on IWT with Tamper Detection for Transferring Electronic Health Record" presented a reversible and lightweight watermarking method for IoT-based healthcare systems employing integer wavelet transform (IWT) and chaotic maps, which is capable of tamper detection [16]. In this study, the authors demonstrated a secure and lightweight watermarking method having imperceptibility and reversibility impacts, with least possible attacks in IoT-based healthcare systems. As per the results, the proposed scheme took advantage of IWT and reduces greatly the computational complexity as compared to other related techniques. Besides, the scheme supports tamper detection and reversibility and is also provably resistant to several signal processing threats.

The research article titled "A Provably Secure Authentication and Key Exchange Protocol in Vehicular Ad Hoc Networks" presents a novel and secure authenticated key agreement scheme to negotiate an agreed session key prior to communicating the confidential information in vehicular ad hoc network (VANET) [17]. In the follow-up of sensing sensitive information, the transmission of information may be affected or tampered due to insecure public wireless channel. Therefore, it becomes critical to secure the transmission. In this context, the proposed protocol achieves the objective by supporting mutual authenticity among the three participating entities including RSU, user, and cloud server. Finally, the formal security analysis depicts that the protocol is workable, efficient, and secure.

The research article titled "Security in Vehicular Ad hoc Networks: Challenges and Countermeasures" discusses the characteristics and all the possible security limitations including attacks and threats at different protocol layers of the VANETs architecture [18]. Moreover, the paper also surveys different countermeasures. This paper surveys VANET security challenges such as DoS, Sybil, impersonation, replay, and other attacks. Furthermore, it presents the possible countermeasures. The survey may serve as a useful reference for future intelligent transport systems.

The research article titled "The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications" presents a comprehensive survey on security and privacy analysis of recent and popular instant messaging applications [19]. In this paper, the authors discussed all the necessary prerequisites that a reader needs to do for securing the messaging applications as well as analyzing the mobile applications that help in implementing end-to-end secure messaging. They define the key characteristics of a secure and privacy-preserving communication protocol for instant messaging apps and then perform an analysis on the most popular ones. Furthermore, the authors perform a comparison on the end-to-end encryption protocols. After the analysis, the authors recommend some possible security improvements for all applications under analysis that provide quite interesting highlights. They use different testing scenarios to study the security and usability characteristics of secure mobile applications and provide suggestions for improvements.

The research article titled "A Reliable Network Intrusion Detection Approach using Decision Tree with Enhanced Data Quality" presents a reliable network intrusion detection approach based on decision tree classifier and engineering feature techniques [20]. In the present research paper, authors proposed a new reliable network intrusion detection approach based on decision tree with improved data quality. The authors employed network data preprocessing and entropy decision-based feature selection to enhance quality of training for building decision tree classifier to boost the quality of intrusion detection. The proposed paper is new and significant because it is based on machine learning algorithm. The experimental study depicts that the contributed approach presents many advantages and shows high accuracy in comparison with other state-of-the-art models.

The research article titled "Internet of Things Security: Challenges and Key Issues" aims to study the key issues including security threats in state-of-the-art IoT-based authentication schemes [21]. Mostly, the paper highlights the current challenges as posed to the induction of IoT devices in the precarious domain. The authors emphasized on securing real and virtual worlds based on IoT technology resulting in secure energy, water management, construction, industry, environment, telecommunications, healthcare, surveillance-based sectors, etc. Mostly, IoT-based networks are prone to Denial of Service (DoS) attack, replay attack, and insider attacks. The authors emphasized on countering the mentioned threats by employing one-time password, elliptic-curve cryptography (ECC), ID-based authentication, and certificate-based authentication solutions.

The research article titled "Adaptive Fault-Tolerant System and Optimal Power Allocation for Smart Vehicles in Smart Cities using Controller Area Network (CAN)"aims to analyze the increased energy consumptions and transmission collisions resulting in loss of data packets in a CAN-based smart vehicle system [22]. The authors try to find the fault-tolerant capability through probabilistic automatic repeat request (PARQ) and also probabilistic automatic repeat request (PARQ) with fault impact (PARQ-FI) and also provide the optimal power allocation in CAN sensor nodes for enhancing the performance of the system. The simulation results depict an increase packet delivery ratio of the proposed scheme. The promising findings of the proposed system may prove to be a significant reference for future smart cities.

The research article titled "Designing an Efficient and Secure Message Exchange Protocol for Internet of Vehicles" aims to present a secure message authenticated key exchange protocol for the exchange of information among legitimate participating members of IoV (SMEP-IoV) [23]. Initially, the author reviewed some of the recently presented authentication protocols for securing IoVs. Then, they constructed a symmetric key-oriented authenticated key exchange protocol which can be employed by a vehicle and corresponding RSU to converge on a mutually agreed secret key with the assistance of vehicle server. The presented SMEP-IoV scheme meets the security as well as performance requirements of IoV. To analyze the security on formal basis, the SMEP-IoV employed BAN logic. According to the demonstrated results, the lightweight SMEP-IoV achieves the desired security properties.

The research article titled "Improved Secure and Lightweight Authentication Scheme for Next-Generation IoT Infrastructure" proposed a secure as well as lightweight authenticated key agreement technique for next-generation IoT infrastructure after reviewing and presenting the weaknesses in Rana et al. [24]. This study suffers from vulnerability to offline password guessing attack and privileged insider threats. The improved scheme solves the drawbacks of reviewed scheme, and its security features are proven under formal as well as informal analysis. They proved the security properties of the scheme using BAN logic as well formal analysis based on the RoR model. Ultimately, they took a comparative analysis of the proposed work and previous related schemes and found that their scheme is not only efficient as far as computational and communicational costs are concerned but also robust regarding the security features. Moreover, the performance evaluation also acknowledges the effectiveness of proposed scheme in terms of time and memory consumption.

The research article titled "AVoD: Advanced Verify-on-Demand for Efficient Authentication against DoS Attacks in V2X Communication" presented a technique for preventing Denial-of-Service (DoS) threats in the interaction of autonomous cooperative driving vehicles by employing security credential management system [25]. The contributed technique minimizes the authentication costs on the basis of classification for similar messages into several categories, while verifying the authenticity for the first message as characterizing the group. This scheme has been duly tested with experiments and demonstrations, while the scheme significantly enhances the speed of processing messages by reducing DoS attacks, attributing to the contributed scheme.

The research article titled "V2X-Based Mobile Localization in 3D Wireless Sensor Network" presented a range-free localization algorithm with respect to sensors in 3D wireless sensor network architecture on the basis of flying anchors [26]. The developed algorithm is quite suitable for localization of the vehicle as it employs the vehicle-to-infrastructure (V2I) based positioning algorithm. It chooses the multilayer C-shaped trajectory for random walk of the mobile anchor-based nodes which is installed with GPS. These anchor nodes keep transmitting beacon signal besides the information of position towards unknown nodes to form a triangle using three further nodes upon receipt of RSSI values. Thereafter, distance is calculated using link quality induction for every mobile anchor node using centroid-based formula for computing localization error. The results of simulation indicate that C-CURVE algorithm demonstrates higher efficiency even in multipath fading. The presented algorithm affords higher accuracy despite the presence of noise, due to the employment of recurring LQI values.

We would like to extend our profound appreciation to all the reviewers and authors for their timely and worthy contributions. Moreover, we would like to thank the Editor-in-Chief of *Security and Communication Networks*, Hindawi, for granting us the privilege to contribute this special issue in the worthy journal. We hope this special issue will provide useful insight to the researchers seeking for the novel prospects to secure vehicular communications.

Conflicts of Interest

The guest editors declare that there are no conflicts of interest regarding the publication of this special issue.

Azeem Irshad
Muhammad Shafiq
Shehzad Ashraf Chaudhry
Muhammad Usman

References

[1] P. Papadimitratos, L. Buttyan, T. Holczer et al., "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[2] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: regulation, research, and remaining challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1858–1877, 2018.

[3] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[4] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[5] R. Hussain, F. Hussain, S. Zeadally, and J. Lee, "On the adequacy of 5G security for vehicular ad hoc networks," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 32–39, 2021.

[6] J. Miao, Z. Wang, X. Miao, and L. Xing, "A secure and efficient lightweight vehicle group Authentication protocol in 5G networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 4079092, 12 pages, 2021.

[7] H. U. Rahman, A. Ghani, I. Khan, N. Ahmad, S. Vimal, and M. Bilal, "Improving network efficiency in wireless body area networks using dual forwarder selection technique," *Personal and Ubiquitous Computing*, vol. 26, no. 1, pp. 11–24, 2022.

[8] X. Li, J. Liu, M. S. Obaidat, P. Vijayakumar, Q. Jiang, and R. Amin, "An unlinkable authenticated key agreement with collusion resistant for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7992–8006, 2021.

[9] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo, and Y. Park, "Robust authentication protocol for dynamic charging system of electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11338–11351, 2021.

[10] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

[11] G. U. Rehman, A. Ghani, M. Zubair, S. A. Ghayyure, and S. Muhammad, "Honesty based democratic scheme to improve community cooperation for Internet of Things based vehicular delay tolerant networks," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4191, 2021.

[12] L. Feng, A. Ali, M. Iqbal et al., "Dynamic wireless information and power transfer scheme for nano-empowered vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4088–4099, 2020.

[13] A. Ghani, A. Badshah, S. Jan, A. A. Alshdadi, and A. Daud, "Issues and challenges in cloud storage architecture: a survey," vol. 12, 2020, https://arXiv.org/abs/2004.06809.

[14] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, and A. Kerrouche, "Implementation of blockchain consensus algorithm on embedded architecture," *Security and Communication Networks*, vol. 20, no. 21, p. 3268, 2021.

[15] M. Azrour, J. Mabrouki, and R. Chaganti, "New efficient and secured authentication protocol for Remote healthcare systems in cloud-IoT," *Security and Communication Networks*, vol. 2021, Article ID 5546334, 12 pages, 2021.

[16] M. Nazari and A. Maneshi, "Chaotic reversible watermarking method based on IWT with tamper detection for transferring electronic health record," *Security and Communication Networks*, vol. 2021, Article ID 5514944, 15 pages, 2021.

[17] T. Y. Wu, Z. Lee, L. Yang, and C. M. Chen, "A provably secure authentication and key exchange protocol in vehicular ad hoc networks," *Security and Communication Networks*, vol. 2021, Article ID 9944460, 17 pages, 2021.

[18] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and Countermeasures," *Security and Communication Networks*, vol. 2021, Article ID 9997771, 20 pages, 2021.

[19] C. Johansen, A. Mujaj, H. Arshad, and J. Noll, "The snowden phone: a comparative survey of secure instant messaging mobile applications," 2018, https://arxiv.org/abs/1807.07952.

[20] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram, "A reliable network intrusion detection approach using decision tree with enhanced data quality," *Security and Communication Networks*, vol. 2021, Article ID 1230593, 8 pages, 2021.

[21] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of things security: challenges and key issues," *Security and Communication Networks*, vol. 2021, Article ID 5533843, 11 pages, 2021.

[22] A. K. Biswal, D. Singh, B. K. Pattanayak, D. Samanta, S. A. Chaudhry, and A. Irshad, "Adaptive fault-tolerant system and optimal power allocation for smart vehicles in smart cities using controller area network," *Security and Communication Networks*, vol. 2021, Article ID 2147958, 13 pages, 2021.

[23] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for Internet of vehicles," *Security and Communication Networks*, vol. 2021, Article ID 5554318, 9 pages, 2021.

[24] C. M. Chen and S. Liu, "Improved secure and lightweight Authentication scheme for next-generation IoT infrastructure," *Security and Communication Networks*, vol. 2021, Article ID 6537678, 13 pages, 2021.

[25] K. Taehyoung, J. Cheongmin, and H. Manpyo, "AVoD: Advanced Verify-on-Demand for efficient authentication against DoS attacks in V2X communication," *Security and Communication Networks*, vol. 2021, Article ID 2890132, 9 pages, 2021.

[26] I. Javed, X. Tang, K. Shaukat et al., "V2X-Based mobile localization in 3D wireless sensor network," *Security and Communication Networks*, vol. 2021, Article ID 6677896, 13 pages, 2021.