EAI/Springer Innovations in Communication and Computing

S Velliangiri
M Gunasekaran
P Karthikeyan *Editors*

Secure Communication for 5G and IoT Networks

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series Editor

Imrich Chlamtac, European Alliance for Innovation, Ghent, Belgium

Editor's Note

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

S. Velliangiri • M. Gunasekaran • P. Karthikeyan
Editors

Secure Communication for 5G and IoT Networks

EAI
RESEARCH MEETS INNOVATION

Springer

Editors
S. Velliangiri
CSE B V Raju Institute of Technology
Narasapur, India

P. Karthikeyan
CSE Jain (Deemed-to-be University)
Bengaluru, India

M. Gunasekaran
Electrical Engineering Technology
University of California
Davis, CA, USA

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-79765-2 ISBN 978-3-030-79766-9 (eBook)
https://doi.org/10.1007/978-3-030-79766-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book highlights state-of-the-art research on secure communication of 5G and the Internet of Things (IoT) Networks, along with related areas to ensure secure and Internet-compatible IoT systems. It discusses 5G and IoT security and privacy challenges and energy-efficient approaches to improve the ecosystems through communication. The book addresses the secure communication and privacy of the 5G and IoT technologies while also revealing the impact of IoT technologies on several scenarios in industrial automation. Intended as a comprehensive introduction, it offers an in-depth analysis. It provides scientists, engineers and professionals with the latest techniques, frameworks and strategies used in 5G and IoT technologies. The book includes intelligent solutions by utilizing artificial intelligence and machine learning to improve the performance of the 5G and IoT security protocols and models. Additionally, this book discusses various applications that use 5G and IoT in multimedia data communications, healthcare and energy.

Narasapur, India — S. Velliangiri
Davis, CA, USA — M. Gunasekaran
Bengaluru, India — P. Karthikeyan

Contents

Chapter 1
Security Challenges in 5G and IoT Networks: A Review

G. Edwin Prem Kumar, M. Lydia, and Yoash Levron

1.1 Introduction

The fifth-generation (5G) networks are destined to emerge as one of the chief drivers of applications and devices involving the Internet of Things (IoT). Wireless technologies have steadily grown from 2G networks supporting only voice, 3G networks for both voice and data, and 4G for broadband connectivity. 4G networks powered by Long Term Evolution (LTE), outperformed all other rival technologies like Bluetooth, Zigbee, Long Range Radio (Lo-Ra) technologies. The challenges faced in 4G in terms of speed, disruptions, and reliability led to the evolution of 5G networks. IoT applications that had already started mushrooming with 3G and 4G networks have set to become the greatest beneficiary of 5G networks. The 5G-based IoT will be able to connect billions of IoT devices and facilitate the implementation of advanced IoT applications like Smart cities, Smart homes, Smart grids, and so on, with this very high-speed connectivity and reliability. The 5G-IoT architecture is expected to be well-coordinated, agile, intelligent, and fully automatic [1]. It would provide enormous number of connections of varying standards and would also implement network functions on-demand, using cloud-based Radio Access Network (RAN). The requirements of 5G-IoT include high data rate, scalability,

G. E. P. Kumar (✉)
Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India

M. Lydia
Department of Mechatronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Y. Levron
The Viterbi Faculty of Electrical Engineering, Technion-Israel Institute of Technology, Haifa, Israel
e-mail: yoashl@ee.technion.ac.il

S. Velliangiri et al. (eds.), *Secure Communication for 5G and IoT Networks*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-79766-9_1

low latency, mobility, battery life, and security. Network function virtualization (NFV), software-defined wireless sensor network (SD-WSN), cognitive radio (CR), and device-to-device (D2D) communications are some of the key enablers in 5G-IoT architecture [2].

The IoT platform comprises of intelligent, heterogeneous devices connected through the internet. The layered architecture of IoT comprises of perception layer, network layer, and application layer. The most common security attacks in the perception layer are interference from radio frequency (RF), jamming of nodes, false node injection, sleep deprivation, and tampering of hardware. Man-in-the-middle attacks, spoofing, sinkhole, and Sybil attacks are common in the network layer and Denial-of-service (DoS), malicious script and phishing attacks take place in the application layer [3]. Insufficient authorization procedures, insecure network services and interfaces, inadequate security configuration, and unreliable communication platforms are some of the attack vectors in IoT systems [4]. Khattak et al. critically reviewed the attacks in the perception layer, which includes attacks in radio frequency identification (RFID), WSN, and RFID sensor network (RSN) [5]. Securing the physical objects in IoT networks has also become an interesting area of research. The physical objects in IoT networks are unpredictable in the spatial and temporal realm, have multiple identities, are resource-constrained, dynamic, highly heterogeneous, and socially aware [6]. These features make securing the IoT product life cycle a big challenging task. An overview of security mechanisms spanning the entire life cycle of IoT products is presented in [7].

As the quantum of connectivity, devices, and coverage is set to reach massive high, serious concerns regarding the security and privacy of the users, devices, and data involved have arisen. The security concerns in 5G-IoT networks must vigilantly consider sealing the cracks and securing weak links in the authentication mechanism, assurance, storage, mobility, and compatibility [1]. Security needs to be ensured both during design and operations, by means of security mechanism, suitable network architectures, and well-tested protocols [8]. Higgins points out that with the integration of 5G and IoT, the risk associated with the innovation is inevitable [9]. Trust levels need to be identified as an important entity in securing the privacy of 5G and IoT networks. Trust models tailor-made for 5G networks, incorporating network slice trust degree concept and facilitating ubiquitous computing is the need of the hour. In a 5G-IoT scenario, challenges like Quality-of-Service, mobility, and slicing stand to gain greater advantage along with fog computing. Sicari et al. concluded that security and privacy constraints in the 5G-IoT scenario need to address issues pertaining to integrity, confidentiality and non-repudiation, intrusion detection, authentication, and access control, key management, trust, and enforcement of policies [10].

With sufficient light thrown on the need for securing the 5G-IoT networks, we continue to discover the technologies for securing the 5G-IoT scenario, the research work carried out on securing the 5G-IoT applications, and the research challenges and avenues to be explored in the future.

1.2 Technologies for Securing 5G-Based IoT Networks

Detection of points, contextual and collective anomalies, network intrusion, malware, ransomware, and intruders are the identified application areas of IoT security. The technologies explored for providing security in the 5G-IoT scenario are presented here (Fig. 1.1).

1.2.1 Authentication and Access Control

Authentication is rendered to be the prime security mechanism in IoT applications. However, these mechanisms have been challenged by attacks like node impersonation, node bypassing, and node capture attacks. Access control involves identification, authentication, authorization, and accountability [5]. Behrad et al. proposed a slice-specific authentication and access control (SSAAC) protocol for a 5G-IoT scenario using three network functions, namely Gateway virtual function provided by a third party, Gateway function repository, and radio resource control connection endpoint [11]. The security aspect of the newly designed RAN was compared with the conventional RAN. Pesic et al. developed the CAAVI-RICS model for securing edge computing platforms [12]. They claimed that the proposed methodology could be used to model most of the attacks in the cyber-physical system. The Credibility,

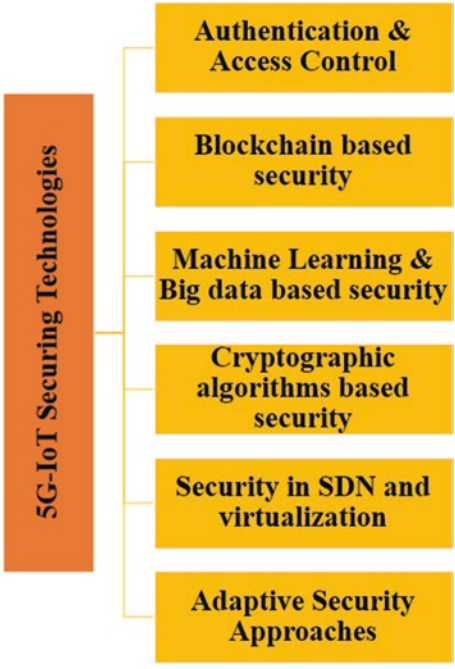

Fig. 1.1 Technologies for securing the 5G-IoT framework

Authentication, Authorization, Verification, and Integrity (CAAVI) model security mechanisms in edge computing platforms would be robust, responsive, dynamic, effective, and resource preserving.

Wazid et al. proposed a lightweight authentication mechanism for a cloud-based IoT environment [13]. The protocol was simulated in NS2 and its effectiveness over other prevailing schemes was analyzed. Patel and Doshi presented a message queueing telemetry transport (MQTT)-based framework for providing validation and access control [14].

1.2.2 Blockchain-Based Security

Adoption of blockchain technology in this 5G-IoT scenario, which usually includes a trusted intermediary, clearly enhances the robustness and trustworthiness of the data involved. A block basically contains the data on transactions, timestamp, cryptographic hash function, reference to the previous block, and smart contracts if required [10]. Blockchain technology provides security based on the transparency of data and auditability, information distribution, robustness, and decentralization. Haris and Al-Madeed presented an exhaustive review on the integration of blockchain technology in a 5G-IoT environment [15]. Qian et al. proposed a novel sophisticated security management algorithm based on blockchain for different layers of IoT architecture [16]. A device identification-based key algorithm was developed based on the interaction between the IoT devices and blockchain database to ensure security and dependability.

1.2.3 Machine Learning and Big Data–Based Security

The machine learning (ML), deep learning (DL), and big data technologies used to secure the IoT services have also been reviewed here. Edge computing platform ushered in the analytics revolution and also enhances the performance of complex applications like virtual and augmented reality, smart city applications, and so on. Establishment of a strong defensive framework and detection of active and passive attacks in IoT networks can be done based on ML techniques, which comprise supervised, unsupervised, and reinforcement learning methodologies [17]. Supervised learning techniques include support vector machine (SVM), random forest (RF), Bayesian theorem, k-nearest neighbor (k-NN), decision tree (DT), neural network (NN), and ensemble learning. Techniques like principal component analysis (PCA) and k-means clustering comprise the unsupervised techniques.

The application of DL and big data technologies for IoT security has been explored in detail by Amanullah et al. [18]. Deep learning architectures including autoencoders, recurrent neural networks (RNN), restricted Boltzmann machine (RBM), deep belief network (DBN), long short-term memory (LSTM), convolution

neural networks (CNN), and so on, can be used for IoT security. Big data technologies like Apache Spark, Apache Hadoop, and Apache Storm along with DL techniques have been used in securing the 5G-IoT net-works especially in the detection of anomalies, node abnormal behavior, and real-time intrusion. He et al. developed an extremely dependable, deep CNN-based multiuser, multi-input multi-output detector for 5G and beyond 5G enabled IoT [19]. The detection performance was increased by incorporating user selection and scheduling criteria. Thantharate et al. proposed a network slicing function based on DL for securing the 5G and beyond 5G networks [20]. The offering of network slicing-as-a-service performed competently with advanced security and dependability, thus resulting in a 'Secure5G' network. Al-Turjman explored the possibility of using big data-based analytics in securing the Internet of Nano-things (IoNT) [21].

1.2.4 Cryptographic Algorithms-Based Security

Traditional cryptographic-based security is highly complex and resource consuming. Hence Kumar et al. developed a lightweight signcryption technique for securing the perception layer in IoT [22]. The proposed scheme used a lightweight hash technique and was proved to be robust and resilient against replay attack, man-in-the-middle attack, impersonation, and device attacks. Dey et al. proposed a methodology based on physical layer key generation and encryption as safety measures [23]. They also explored the efficacy of advanced encryption standard (AES) and compared it with other methods and concluded that the AES algorithm outperformed the other algorithms. El-Latif et al. proposed two effective quantum-based hash functions and security protocols for protecting data in 5G networks [24]. The proposed quantum-based security algorithm outperformed the existing methods and proved to be robust against a man-in-the-middle attack, measurement attack, and message attack.

1.2.5 Security in Software-Defined Framework and Virtualization

5G-IoT scenario is largely based on software-defined network (SDN) and network function virtualization (NFV). Sethi et al. proposed a secure self-optimized SDN framework for narrow band-IoT in 5G networks [25]. An exhaustive review on the security framework in virtualized 5G networks was carried out by Suraci et al. [26]. The security risks and threats underlying the 5G landscape were analyzed from the stakeholders' point of view. Shafi et al. analyzed the security threats in novel technologies incorporated in 5G-IoT scenarios like device-to-device communication, spectrum sharing, ultra-dense networks, and so on [27]. They also analyzed the 5G–New Radio security issues from the aspect of artificial rain and dust.

1.2.6 Adaptive Security Approaches

In resource-constrained networks, adaptive security approaches have proven to be successful to offer energy-efficient security. These approaches are generally classified into data-centric approaches and threat-centric approaches. Data-centric approaches examine the sensitivity of the data involved and adapt the security methodology whereas the threat-centric approach examines the threats involves and adapts accordingly. Hellaoui et al. proposed an end-to-end adaptive approach for an energy-efficient solution in securing the 5G-based IoT [28].

1.3 Securing the 5G-Based IoT Applications

This section presents a brief overview of the various 5G-based IoT applications and the security mechanisms incorporated in these (Fig. 1.2).

1.3.1 Securing the Smart Grid

Smart Grid (SG) is chiefly an automated power delivery network, with improved protection, reliability, and efficient monitoring. Hui et al. conducted an exhaustive survey on the 5G-IoT scenario for demand response in SG networks. Application of

Fig. 1.2 Securing the 5G-IoT applications

5G-IoT aids in robust security, high-speed transfer of data, massive increase in connection of flexible loads, and enhanced reliability in SG networks [29]. Borgaonkar and Jaatun analyzed the implementation of secure IoT in SG networks [30]. They presented the benefits of 5G in two types of IoT devices, namely regular IoT devices like drones, connected cars, and so on, and small resource inhibited remotely placed sensors and actuators. They concluded by formulating technical principles to be adhered to for ensuring layer-based security in SG networks.

1.3.2 Securing the Smart Home

Smart homes promise increased comfort and a sophisticated lifestyle. However, the issue of security and problems of cybersecurity remains a serious undeniable threat. Wasicek has pointed out that micro-segmentation in 5G smart homes is a promising area to be explored to ensure security [31]. Jha et al. proposed layer-wise security for smart home applications [32]. They mathematically modeled the security of a smart home system, assessed the secrecy capacity and outage probability to tackle layer-wise security attacks.

1.3.3 Securing the Intelligent UAV

Unmanned aerial vehicles (UAV) have found application in several areas. Nomikos et al. proposed a mobile 5G RAN based on UAV to enable immense connectivity between IoT devices and mobile users. They analyzed the security threats in flying ad-hoc networks (FANETs) and concluded that independent behavior, self-organization, anonymity, and lack of fixed infrastructure are among the chief causes that affect its security [33]. Wang et al. proposed a novel methodology to guarantee secure and effective data aggregation in UAVs [34]. The proposed secure methodology known as the Intelligent UAV-based Data Aggregation algorithm (IDAA) outperformed the conventional techniques.

1.3.4 Securing the VANET

Intelligent transportation system has been greatly benefitted by the 5G-IoT scenario. However, the security challenges faced by Vehicular Ad-hoc Networks (VANETs) have also multiplied. Xie et al. proposed a trustworthy solution for 5G-VANETs based on blockchain technology [35]. The efficacy of the proposed methodology was validated with regard to user security, malicious vehicle analysis, and compromised roadside units. Al-Turjman and Lemayian presented a comprehensive overview on securing the VANETs [36]. They categorized the

attacks on vehicle sensor networks as physical attacks, side-channel attacks, environmental attacks, cryptoanalysis attacks, software, and network attacks. Hussain et al. presented a review on the amalgamation VANETs and 5G security [37]. According to them, the 5G threat landscape included 5G core network protection, 5G cloud RAN protection, threats in the device or the end-user, and threats in business application.

1.3.5 Securing the Smart City

5G and IoT infrastructures are definitely a great asset for the reliable functioning of smart cities. Securing the smart city application is also a challenging task. Serrano proposed a combination of blockchain techniques with random neural networks for ensuring cybersecurity in the 5G-IoT networks [38]. The developed model was proved to provide security to all the layers of the 5G networks and node authentication in smart buildings. Godquin et al. developed a methodology to optimally position security solutions using graph theory [39]. The proposed technique was validated for smart city infrastructure.

1.3.6 Securing the Smart Factory

The penetration of 5G-IoT networks has revolutionized industries and the manufacturing process. It has resulted in smart interconnection of shop floors, application of big data analytics, cloud computing, virtual and augmented reality, and smart manufacturing. Cheng et al. analyzed the security requirements in 5G integrated smart manufacturing [40]. The application of blockchain technique in securing the 5G-enabled IoT in industries was put forth by Mistry et al. [41]. They have presented a comprehensive review and analyzed the problems and solutions in smart factories.

1.3.7 Securing the Smart Health

The healthcare industry has witnessed a tremendous change with the advent of 5G wireless networks and IoT. There has been an evolution in the development of scalable, dependable, and secure protocols and architectures for data acquisition, transmission, and storage from body sensors [42]. 5G-IoT networks have been a great boon to Sports Health monitoring as well [43]. Minahil et al. proposed an elliptic curve cryptography-based authentication protocol for e-health clouds [44]. The

methodology was lightweight and was proved to outperform conventional techniques in terms of computational complexity and robustness.

1.3.8 Security in Other Applications

Financial Innovation

5G-IoT networks are poised to impact the financial sector as well. Cheng has pointed out that secure protocols can pave the way to noteworthy trade cycles and reduce transaction delays [45]. It can lay the platform for innovation in smart rural finance.

Environment

5G-enabled IoT networks play an important role in environmental aspects too. Han et al. proposed a blockchain-based secure architecture for monitoring and measurement of air pollution [46].

Smart Agriculture

5G-based IoT networks play a critical role in smart and precision farming too. Tang et al. presented an exhaustive survey on the role of 5G networks in agriculture and the need for a secure communication channel, connectivity, and storage [47].

1.4 Research Challenges in Securing 5G-IoT Networks

The research works pertaining to technologies involved in securing 5G-IoT networks have been summarized in Table 1.1. The various issues that continue to challenge researchers in the area of 5G-IoT security have been presented in this section.

1.4.1 Challenges Related to 5G-IoT Architecture

Scalability, heterogeneity, and interoperability continue to remain a challenge in 5G-IoT architecture. Standardization has gained much significance as 5G-IoT has evolved as a very complex ecosystem. The need to conform to both technology and regulatory standards is a challenging task yet to be addressed. There is an increasing need for the development of novel transmission techniques based on the distance

Table 1.1 Securing technologies applicable to 5G-IoT—a summary

Securing technology	Proposed mechanism
Authentication and Access Control (AAC)	Slice Specific AAC [11]
	CAAVI-RICS [12]
	Lightweight Authentication Mechanism [13]
	Novel MQTT security framework [14]
Blockchain-based security	Decentralized IoT security [16]
Machine Learning and Big data-based security	DL-based ultrareliable multiuser, multi-input, multi-output detector [19] DL-based model for robust network slicing framework [20]
Cryptographic algorithms based security	Lightweight signcryption method [22] Physical layer key generation and encryption [23] Quantum-based security protocol [24]
Security in SDN and virtualization	5G SoftAir architecture
Adaptive security	Coalition game algorithm with trust evaluation [28]

and bandwidth of transmission. The impact of path loss and noise needs to be analyzed meticulously.

1.4.2 Challenges Related to Blockchain Technologies

Block mining in Blockchain technology consumes a lot of energy and is computationally complex. This technology is also memory intensive and power consuming.

Maintaining security and privacy in every smart application is a major open research challenge. Preserving confidentiality, integrity, and authenticity of data and users need to be ensured by the incorporation of suitable cryptographic algorithms or trust levels. Development of compatible protocols for securing the IoNT is also an area to be explored. Security in ubiquitous data aggregation and visualization, state estimation, and distribution networks in SG networks is a required area of research. In VANETS, secure positioning, secure data acquisition, and verification, secure routing and delay have emerged as potential areas of research.

1.4.3 Challenges Related to Energy

Deficiency in standardization, increase in energy consumption and lower storage capacity and computational power are some of the challenges that need to be explored in 5G-enabled IoT applications. Energy-efficient solutions and viable NFV are the need of the hour. Research in energy-efficient protocols and spectrum harvesting techniques is a key trend yet to be explored in a big way. Solutions that are context-aware and convergent are needed.

1.4.4 Challenges Related to Artificial Intelligence

Artificial Intelligence (AI) based solutions for abnormal traffic monitoring is an emerging research area in 5G-IoT networks. Designing an effective traffic detection solution in IoT is a real challenge. Diverse devices in IoT have made identification a major issue. AI- and ML-based solutions of identity verification are a major challenge in 5G-IoT networks. Integration of AI with blockchain technology is also an open area of research. Authentication of training datasets is a significant challenge in ML-based security solutions.

1.4.5 Challenges Related to Software Defined Networks

The efficacy of software-defined framework in the 5G-IoT scenario needs to be ascertained. Securing SDN is also a research challenge. The trade-off between the performance of the SDN and its security poses a significant test. Evolving hybrid SDN control architecture for 5G-IoT networks is also an emerging research area.

1.5 Conclusion

Accurate detection of security threats, optimum computational and time complexity, reduced energy constraint, and security at edge computing platforms are the chief requirements of any security algorithm. This chapter presents an exhaustive review on authentication and access control protocols, key management, trust management, and intrusion detection systems for 5G and IoT networks. The role of edge computing and blockchain technology in incorporating security to 5G networks has also been explored. Since security and privacy methodologies are generally complex and resource-intensive, energy-efficient, effective and lightweight compatible solutions are the need of the hour. 5G will definitely be a great enabler in making the IoT smarter and ubiquitous. The research challenges presented give a better and in-depth insight into the need for securing 5G-IoT networks.

References

1. Li S, Xu LD, Zhao S (2018) 5G Internet of Things: A Survey. J. of Indus. Inform. Integ. 10: 1–9.
2. Shafique K, Khawaja BA, Sabir F, Qazi S, Mustaqim M (2020) Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access 8: 23022–23040.
3. Yugha R, Chithra S (2020) A survey on technologies and security protocols: Reference for future generation IoT. J. of Network and Computer Applications 169: 102763.

4. Noor MBM, Hassan WH (2019) Current research on Internet of Things (IoT) security: A survey. Computer Networks 148: 283–294.
5. Khattak HA, Shah MA, Khan S, Ali I, Imran M (2019) Perception layer security in Internet of Things. Future Generation Computer Systems 100: 144–164.
6. Yao X, Farha F, Li R, Psychoula I, Chen L, Ning H (2020) Security and privacy issues of physical objects in the IoT: Challenges and opportunities. Digital Communications and Networks. In Press (Available Online)
7. Yousefnezhad N, Malhi A, Framling K (2020) Security in product lifecycle of IoT devices: A survey. J. of Network and Computer Applications 171: 102779.
8. Mazurczyk W, Bisson P, Jover RP, Nakao K, Cabaj K (2020) Special issue on Advancements in 5G Networks Security, Future Generation Comp. Sys. 110: 314–316.
9. Higgins D (2020) Innovation and risk walk hand-in-hand with 5G and IoT. Network Security, 16–18.
10. Sicari S, Rizzardi A, Coen-Porisini A (2020) 5G in the internet of things era: An overview on security and privacy challenges. Computer Networks 179: 107345.
11. Behrad S, Bertin E, Tuffin S, Crespi N (2020) A new scalable authentication and access control mechanism for 5G-based IoT. Future Generation Comp. Sys. 108: 46–61.
12. Pesic S, Ivanovic M, Radovanovic M, Badica C (2020) CAAVI-RICS model for observing the security of distributed IoT and edge computing systems. Simulation Modelling Practice and Theory 105: 102125.
13. Wazid M, Das AK, Bhat V, Vasilakos AV (2020) LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. J. Network and Computer Applications 150: 102496.
14. Patel C, Doshi N (2020) A novel MQTT security framework in generic IoT model. Procedia Computer Science 171: 1399–1408.
15. Haris RM, Al-Maadeed S (2020) Integrating Blockchain Technology in 5G enabled IoT: A Review. IEEE Intl. Conf. on Informatics, IoT and Enabling Technologies, 367–371.
16. Qian Y, Jiang Y, Chen J, Zhang Y, Song J, Zhou M, Pustisek M (2018) Towards decentralized IoT security enhancement: A block-chain approach. Computers and Electrical Engg. 72: 266–273
17. Tahsien SM, Karimipour H, Spachos P (2020) Machine learning based solutions for security of Internet of Things (IoT): A survey. J. of Network and Computer Applications 161: 102630.
18. Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ah-med E, Nainar ASM, Akim NM, Imran M (2020) Deep learning and big data technologies for IoT security. Computer Communications 151: 495–517.
19. He K, Wang Z, Li D, Zhu F, Fan L (2020) Ultra-reliable MU-MIMO detector based on deep learning for 5G/B5G-enabled IoT. Physical Communication 43: 101181.
20. Thantharate A, Paropkari R, Walunj V, Beard C, Kankariya P (2020) Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond. 10th Annual Computing and Communication Workshop and Conference, 0852-0857
21. Al-Turjman F (2020) Intelligence and security in big 5G-oriented IoNT: An overview. Future Generation Computer Systems 102: 357–368.
22. Kumar A, Saha R, Alazab M, Kumar G (2020) A Lightweight Signcryption Method for Perception Layer in Internet-of-Things. J. of Information Security and Applications 55: 102662.
23. Dey A, Nandi S, Sarkar M (2018) Security measures in IoT based 5G networks. 3rd International Conference on Inventive Computation Technologies, pp. 561–566.
24. El-Latif AAA, Abd-El-Atty B, Andraca SEV, Mazurczyk W (2019) Efficient quantum-based security protocols for information sharing and data protection in 5G networks. Future Generation Computer Systems 100: 893–906.
25. Sethi A, Jain SK, Vijay S (2020) Secure self-optimizing soft-ware defined framework for NB-IoT toward 5G. Procedia Computer Science 171: 2740–2749
26. Suraci C, Araniti G, Abrardo A, Bianchi G, Iera A (2021) A stakeholder-oriented security analysis in virtualized 5G cellular networks. Computer Networks 184: 107604.

27. Shafi M, Jha RK, Sabraj M (2020) A survey on security issues of 5G NR: Perspective of artificial dust and artificial rain. J. of Network and Computer Applications 160: 102597.
28. Hellaoui H, Koudil M, Bouabdallah A (2020) Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach. IEEE Internet of Things Journal 7 (7): 6589–6602.
29. Hui H, Ding Y, Shi Q, Li F, Song Y, Yan J (2020) 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. Applied Energy 257: 113972.
30. Borgaonkar R, Jaatun MG (2019) 5G as an enabler for secure IoT in the Smart Grid. First Intl. Conf. on Societal Automation, 1–7.
31. Wasicek A (2020) The future of 5G smart home network security is micro-segmentation. Network Security 11: 11–13
32. Jha RK, Puja, Kour H, Kumar M, Jain S (2021) Layer based security in Narrow Band In-ternet of Things (NB-IoT). Computer Networks 185: 107592.
33. Nomikos N, Michailidis ET, Trakadas P, Vouyioukas D, Karl H, Martrat J, Zahariadis T, Papadopoulos K, Voliotis S (2020) A UAV-based moving 5G RAN for massive connectivity of mobile users and IoT devices. Vehicular Communications 25: 100250.
34. Wang X, Garg S, Lin H, Kaddoum G, Hu J, Alhamid MF (2021) An Intelligent UAV based Data Aggregation Algorithm for 5G-enabled Internet of Things. Computer Networks 185: 107628.
35. Xie L, Ding Y, Yang H, Wang X (2019) Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. IEEE Access 7: 56656–56666
36. Al-Turjman F, Lemayian JP (2020) Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. Computers and Electrical Engineering 87: 106776.
37. Hussain R, Hussain F, Zeadally S (2019) Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems 101: 843–864.
38. Serrano W (2021) The Blockchain Random Neural Network for cybersecure IoT and 5G infrastructure in Smart Cities. J. of Network and Computer Applications 175: 102909.
39. Godquin T, Barbier M, Gaber C, Grimault JL, Bars JML (2020) Applied graph theory to security: A qualitative placement of security solutions within IoT networks. J. Information Security and Ap-plications 55: 102640
40. Cheng J, Chen W, Tao F, Lin CL (2018) Industrial IoT in 5G environment towards smart manufacturing. J. of Indus. Information Integ. 10: 10–19.
41. Mistry I, Tanwar S, Tyagi S, Kumar N (2020) Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical Systems and Signal Processing 135: 106382.
42. Rodrigues JJPC, Zeadally S, Kumar N (2017) Special Issue on 5G Wireless Networks for IoT and Body Sensors. Computer Networks 129: 335–339.
43. Zhan K (2021) Sports and Health Big Data System Based on 5G Network and Internet of Things System. Microprocessors and Microsystems 80: 103363.
44. Minahil, Ayub MF, Mahmood K, Kumari S, Sangaiah AK (2021) Lightweight authentication protocol for e-health clouds in IoT based applications through 5G technology. Digital Communications and Networks 7(2): 235–244.
45. Cheng K (2020) Smart Rural Financial Innovation based on 5G Network and Internet of Things. Microprocessors and Microsystems: 103500, In Press.
46. Han Y, Park B, Jeong J (2019) A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications. Procedia Computer Science 155: 728–733.
47. Tang Y, Dananjayan S, Hou C, Guo Q, Luo S, He Y (2021) A survey on the 5G network and its impact on agriculture: Challenges and opportunities. Computers and Electronics in Agriculture 180: 105895.

Chapter 2
Energy-Efficient Network Routing Protocols for IoT Applications

Deepa Devassy, Immanuel Johnraja Jebadurai, Getzi Jeba Leelipushpam Paulraj, Salaja Silas, and Jebaveerasingh Jebadurai

2.1 Introduction

IoT takes part a crucial part in our routine life [1]. IoT describes a network that consists of various items that are capable of interacting with each other. Every object contains various components such as sensors, actuators, processors, and transceivers to sense and process the data. Large numbers of such devices called nodes are deployed around the world of the Internet [2].

Every device in the network is connected to its nearest base station either directly or indirectly. In a single-hop network, the nodes are right away joined to the base station, whereas in a multi-hop network, the chunks of packets travel through multiple links to land at the base station. The data packets experience various kinds of delay en route. As the packets travel through the nodes, they process the packet and forward it to the destination. This phenomenon is called routing.

This paper provides an insight into various algorithms and protocols used for routing in IoT. Routing is an energy-intensive process in any node. Improper selection of routing algorithms impacts network lifetime. Hence, the selection of suitable routing algorithms plays a vital role to guarantee network performance. A detailed study of various routing protocols has been carried out and their performance is compared with various parameters such as hop count, network scalability, end to end delay, energy consumption, and packet loss rate. The applicability of those protocols in the IoT environment has also been studied and presented in this paper.

The remainder of this chapter is arranged as follows. Section 2.2 details various issues and challenges in IoT. Section 2.3 presents the classification of various

D. Devassy (✉)
Karunya Institute of Technology and Sciences, Coimbatore, India

I. J. Jebadurai · G. J. L. Paulraj · S. Silas · J. Jebadurai
Department of CSE, Karunya Institute of Technology and Sciences, Coimbatore, India
e-mail: getzi@karunya.edu

S. Velliangiri et al. (eds.), *Secure Communication for 5G and IoT Networks*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-79766-9_2

routing protocols. Section 2.4 addresses the analysis of prominent clustering routing protocols. Section 2.5 identifies various research platforms and tools used in the field of networks. Finally, Sect. 2.6 completes the chapter with future research discussions.

2.2 Issues and Challenges in IoT

IoT in its inherent characteristics poses heterogeneous characteristics. These characteristics include context awareness, scalability, energy consumption, low-powered devices, heterogeneity, network connectivity, mobility, security, load balancing, and congestion control. Insights into these parameters are presented in the following subsection.

- Context awareness
- The context refers to the collected information from any location. The factors such as temperature, pressure, and humidity can be measured through various sensors to determine the context [3]. Then the device analyses the contextual facts provincially to elect the pathway that finest fits the prerequisite of a specified exercise. This type of routing protocol faces mass hurdles all along with information exchange, inclusive of lower delay, larger reliability on data transmission, and least power dissipation.
- Scalability
- Usage of embedded systems in IoT extends huge deployment of tiny devices such as sensors and actuators in online applications. The volume of data generated and bandwidth required, grow unboundedly with the increment in the number of these devices. Hence data management and device management are other difficulties in IoT [4].
- Energy Consumption
- The battery power of electronic components in IoT is drained while transporting data. In view of energy constraint, a tradeoff between the quality of information gained and energy consumption by IoT systems is to be retained. Furthermore, the existence of any resource in IoT relies on the availability of energy. The lack of energy prompts the complete habitat under monitoring. Therefore, there is a remarkable longing to lower energy exploitation for the continued lifespan of resources and the well-planned operation of IoT systems [5].
- Low powered devices
- Novel approaches in telecommunications have granted the design of microchips, which can be linked to the Internet, licensing a new era of Internet-of-things (IoT) [6]. These devices run with either a rechargeable or non-rechargeable battery. It is very essential to maintain the power of these devices, otherwise more nodes will go to an inactive stage, which are called dead nodes. Hence it is very essential to maintain the energy of these low-powered devices in IoT.
- Heterogeneity

- IoT networks allow the communication of a variety of devices using different protocols and standards for different applications. All these devices are heterogeneous [7] in hardware design and specification. Data generated from these devices is also heterogeneous in nature [8]. Hence robust methodologies are required to process and use them.
- Network Connectivity
- Quick connectivity of networks and context-aware arithmetic with network resources is the life of IoT [9]. In IoT, billions of devices are assigned with specific addresses, which are connected worldwide through the internet. This connectivity allows devices to exchange information based on some set of standard communication protocols. Maintaining the connectivity of devices is another major challenge in IoT [10].
- Mobility
- Devices or the nodes connected to the IoT network may be static or mobile. Mobility allows the devices to move around different places [11]. This opens another challenge in IoT implementations. When one device moves from one gateway to another, there are chances of interruption in its service. Hence, the system has to adopt mobility management schemes to provide users with QoS under any network condition. Various mobility mechanisms for ad hoc networks are motivated by birds flying in flocks [12].
- Security and Privacy
- This parameter is not fully addressed in IoT by virtue of the open nature of communication in sensor networks. Networks are more vulnerable to various attacks. Thus, this parameter has vital importance in wireless communication [13]. Security based on DTLS and two-way authentication [14], a technique based on elliptic curve cryptography [15] are some of the secure examples adopted in IoT, which are vulnerable to attack. Hence, some mechanisms to be adopted to ensure security to the data, which is being transmitted using Wi-Fi networks.
- Load balancing
- The exponential growth of IoT devices leads to edge computing. The data is being stored into the cloud as well as retrieved from the cloud. Enormous amount of data is being generated during the course of these devices. Load conditions can fluctuate explosively. Thereby a proper load balancing amidst edge servers is required. Under heavy traffic congestion, distribution of load equally to the edge servers is a major concern [16].
- Congestion Control
- Congestion occurs when more data appears in the network. This causes the dropping of packets or delay in the data transmission. Hence appropriate congestion control mechanisms have to be adopted in various layers of the network model for congestion control [17].

2.3 Classification of Routing Protocols in IoT

Protocols work in sensor networks and wireless networks may be adopted for IoT environments with necessary modifications. This section describes different traits of routing protocols existing in IoT. Routing protocols are mainly classified based on four functionalities. They are packet forwarding, route discovery, routing schemes, and routing operations. Figure 2.1 shows the taxonomy of routing protocols in IoT.

2.3.1 Packet Forwarding

Packet forwarding methods are classified into two. They are

- Hop-by-hop routing: Here, the packets take routes available in the forwarding table of all the nodes. Routing table is updated when the packets travel through it. Each node keeps up a routing table with its incoming and outgoing connections. This link information is updated as and when the network topology changes. The data packet contains only the destination information in its header. Based on this, the link with the least cost metric is selected as the next hop. Thus, it guarantees the network bandwidth [18] by properly allocating the resources.
- Source routing: In source routing [19], the entire route information is being held in the header of every packet. The network resources are already allocated prior to the transmission.

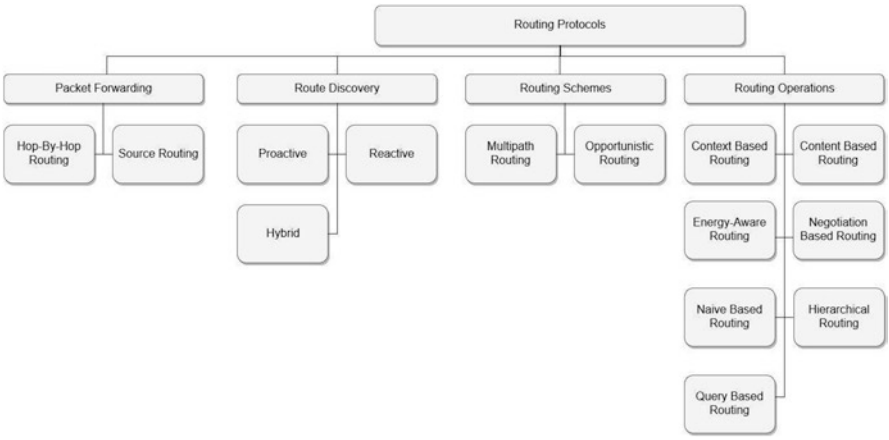

Fig. 2.1 Taxonomy of routing protocols