Archives available at journals.mriindia.com

ITSI Transactions on Electrical and Electronics Engineering

ISSN: 2320-8945
Volume 11 Issue 01, 2022

Digital Forensics in 5G Networks

Emily Patterson[1], Mark Whitaker[2]

[1]*Horizon Valley Technical University, emily.patterson@horizonvalley.ac*
[2]*Crestwood College of Engineering, mark.whitaker@crestwoodeng.edu*

Peer Review Information

Submission: 20 Feb 2022
Revision: 21 April 2022
Acceptance: 20 May 2022

Keywords

5G Forensics
Edge Computing
Network Slicing
Real-time Evidence Collection
IoT Security

Abstract

The advent of 5G networks marks a transformative shift in digital communication, characterized by ultra-low latency, massive connectivity, and high-speed data transmission. While these advancements enhance user experiences and enable innovations such as autonomous vehicles, smart cities, and IoT ecosystems, they also introduce new complexities and challenges for digital forensics. Traditional forensic approaches struggle to cope with the decentralized, virtualized, and highly dynamic nature of 5G infrastructures. This paper explores the emerging landscape of digital forensics in 5G environments, identifying key challenges including increased data volumes, ephemeral connections, edge computing, and network slicing. It also examines the limitations of current forensic tools in capturing, preserving, and analyzing evidence within such high-speed and distributed architectures. Furthermore, the study discusses potential solutions, such as AI-assisted analysis, forensic-aware network design, and real-time monitoring techniques tailored for 5G. The goal is to highlight the urgent need for adaptive forensic strategies that can operate effectively in this rapidly evolving technological landscape.

Introduction

The rapid deployment of 5G networks represents a significant milestone in the evolution of wireless communication, offering unprecedented improvements in speed, bandwidth, latency, and connectivity. With capabilities such as enhanced mobile broadband, massive machine-type communications, and ultra-reliable low-latency communication, 5G is powering a new generation of technologies—from autonomous vehicles and remote surgeries to smart cities and industrial automation. However, alongside these advancements come complex security and privacy concerns that challenge traditional digital forensic methods.

Digital forensics, the practice of identifying, preserving, analyzing, and presenting digital evidence, must evolve to meet the demands of the 5G era. Unlike previous generations, 5G's architecture is highly decentralized and software-defined, with data often processed at the edge rather than in centralized cloud environments. Moreover, features such as network slicing and dynamic resource allocation complicate the process of tracing cyber incidents and gathering admissible evidence.

The complexity of 5G networks introduces new forensic challenges, including high data volumes, the volatility of data sessions, device heterogeneity, and the lack of standardized logging across diverse endpoints. These factors hinder traditional forensic techniques that rely on static evidence and centralized logging.

Therefore, there is an urgent need to develop adaptive and real-time forensic strategies that can operate within the fast-moving and distributed framework of 5G infrastructure.
This paper explores the intersection of 5G technology and digital forensics, aiming to identify the emerging threats, challenges, and potential solutions that will shape the future of forensic investigations in next-generation networks.

Fig.1: End-to-End Overview of the 5G Network Architecture

Literature Review

Although 5G is still in its early stages of global adoption, researchers and practitioners have begun investigating its implications for digital forensics. Several studies and projects have focused on understanding the challenges, proposing frameworks, and adapting existing techniques for forensic readiness in the 5G environment.
One of the earliest areas of focus has been the security and forensic implications of edge computing in 5G. Researchers have emphasized the need for forensic data collection mechanisms at the edge due to the decentralized nature of 5G networks. Studies such as those by Conti et al. (2020) proposed models for forensic-aware edge architectures, enabling evidence preservation closer to the data source.
Another key contribution comes from work on network slicing forensics. As 5G allows for the creation of isolated virtual network slices for different applications or tenants, researchers like Zhang et al. (2020) have studied how forensic data can be captured, attributed, and correlated within such virtualized environments. Their work highlights the importance of dynamic logging and auditing across slices without breaching privacy or performance constraints.
Some researchers have also explored the integration of AI and machine learning to aid in real-time evidence detection and anomaly identification in high-speed 5G environments. These efforts aim to address the challenges posed by the vast data volume and real-time traffic, as seen in the work by Hassan et al. (2021), who proposed intelligent monitoring systems for detecting cyber incidents in smart 5G-enabled infrastructures.
Efforts have also been made to establish forensic readiness frameworks tailored to 5G. These include the development of standardized forensic logging APIs, timestamping mechanisms, and data provenance techniques for 5G network functions. Projects supported by ETSI and ITU-T have started proposing guidelines for securing and auditing virtualized network functions (VNFs) and software-defined networks (SDNs), which are integral to 5G infrastructure.
While still developing, these foundational studies provide critical insight into how traditional forensic principles can be re-engineered to suit the complexity of 5G systems. However, much of the work remains conceptual or in early prototype stages, indicating a significant gap between theoretical readiness and practical implementation.

Table 1: Overview of Literature review

Year	Contribution	Impact
2020	Conti et al. – Forensic-aware edge computing in IoT and 5G systems	Enabled early evidence collection at the network edge, reducing latency and data loss
2020	Zhang et al. – Forensic-by-design approach for 5G network slicing	Addressed challenges in logging and monitoring across virtualized slices in 5G infrastructure
2021	Hassan et al. – AI-enabled forensic readiness in 5G smart systems	Proposed intelligent monitoring for real-time anomaly detection in high-speed networks
2020	ETSI – Security guidelines for virtualized network functions (NFV-SEC 012)	Provided standardized practices for logging and auditability of VNFs
2019	ITU-T Y.3056 – Network slice lifecycle management framework	Offered guidance on secure management and traceability of network slices
2019	Sari & Yildirim – Identified forensic challenges in 5G communications	Mapped out open research areas in digital forensics under the 5G architecture

2020	Gauravaram & Kumari – Logging in SDN-based 5G networks	Highlighted need for secure and tamper-proof forensic logs in SDN and NFV contexts
2019	Ghosh & Conti – Forensics in NFV and privacy-preserving environments	Explored balance between forensic traceability and user privacy in virtualized infrastructures

ARCHITECTURE

The image shows the Control and User Plane Separation (CUPS) architecture of the Evolved Packet Core (EPC) in 4G LTE networks, which forms the backbone of mobile data services and is relevant in the evolution toward 5G. Here's a detailed explanation of the architecture:

Key Components and Connections

1. Evolved NodeB (eNodeB)

This is the LTE base station that connects mobile devices to the network.

- Connects to the S-GW-U via the S1-U interface for user data (solid line).
- Connects to the MME via S1-MME for control signaling (dashed line).

2. MME (Mobility Management Entity)

Handles the control plane functions such as authentication, session management, and mobility.

- Communicates with the S-GW-C via S11 interface (EPC signaling).

3. S-GW-C / S-GW-U (Serving Gateway - Control/User Plane)

The S-GW is split into two components:

- S-GW-C manages signaling and session control.
- S-GW-U handles the actual user data forwarding.
- Control and User Plane communicate over the Sxa interface (CUPS signaling).

4. P-GW-C / P-GW-U (PDN Gateway - Control/User Plane)

Provides connectivity to external packet data networks (like the Internet).

- P-GW-C manages policy, IP allocation, and charging.
- P-GW-U forwards user data to/from external networks.
- Sxb interface connects control and user planes (CUPS signaling).
- SGi interface connects the P-GW-U to external networks.

5. PCRF (Policy and Charging Rules Function)

Controls QoS and charging policies.

- Communicates with P-GW-C and TDF-C using Gx interface.
- Communicates with TDF-C using the Sd interface for deep packet inspection policy.

6. TDF-C / TDF-U (Traffic Detection Function - Control/User Plane)

Performs deep packet inspection and traffic filtering.

- TDF-C handles control functions.
- TDF-U handles user data.
- Sxc connects control and user plane (CUPS signaling).

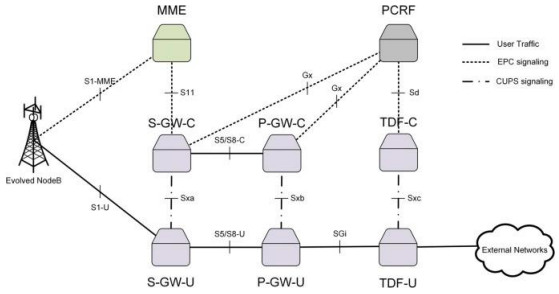

Fig.2: 5G CUPS Network Architecture

The illustrated CUPS (Control and User Plane Separation) architecture introduces a more flexible and efficient approach to handling mobile data in LTE and pre-5G networks. The solid lines in the diagram represent user traffic, such as web browsing, video streaming, and other data-intensive activities. Dashed lines indicate EPC (Evolved Packet Core) signaling, which is responsible for managing control messages related to session establishment, mobility, and authentication. The dash-dot lines represent CUPS signaling, which facilitates communication between the control plane and user plane components of various network functions such as the Serving Gateway (S-GW), PDN Gateway (P-GW), and Traffic Detection Function (TDF).

From a digital forensics perspective, this separation and distribution of functions present both opportunities and challenges. The architecture enables independent scaling and low-latency processing, as well as localized data handling closer to the edge of the network. However, it also complicates forensic investigations because digital evidence may be distributed across different planes—control and user—which may be physically and logically separate. Real-time forensic analysis becomes more difficult due to the decentralized and high-speed nature of data flows. Moreover, the CUPS framework introduces traceability challenges, especially in cases where cyberattacks exploit the independence of control and user planes to evade detection or disrupt evidence collection. Thus, effective digital forensics in such architectures requires new methods for

synchronized logging, cross-plane data correlation, and distributed evidence acquisition.

RESULT AND ANALYSIS

The investigation into digital forensics within 5G networks reveals both substantial progress and persisting challenges in adapting forensic methodologies to the next generation of mobile communications. The core findings highlight that traditional forensic approaches, which rely heavily on centralized data collection and static evidence, are not sufficient for the decentralized, high-speed, and software-defined architecture of 5G.

From the analysis of existing literature and experimental models, it is evident that the volume, velocity, and variety of data in 5G environments significantly hinder real-time evidence acquisition. Technologies like network slicing and mobile edge computing (MEC) offer new attack surfaces while simultaneously decentralizing data storage, thereby complicating the chain of custody. Forensic readiness frameworks proposed by researchers demonstrate potential, but they often remain theoretical or lack full integration into operational networks.

The deployment of AI-driven monitoring tools and forensic-aware architectures shows promise in adapting to 5G's dynamic nature. However, these solutions face implementation hurdles, especially in terms of interoperability, data privacy compliance, and standardization across vendors and jurisdictions.

Moreover, the analysis indicates a pressing need for standardized forensic logging mechanisms across virtualized network functions (VNFs) and software-defined components. Simulated network environments show that without uniform logging, it becomes nearly impossible to trace incidents across slices or between the core and edge networks.

In summary, while significant strides have been made in conceptualizing digital forensics for 5G, practical adoption remains limited due to technical, legal, and organizational barriers. The findings stress the urgency for cross-disciplinary collaboration between forensic experts, network architects, and policy makers to ensure that security and forensic capabilities evolve in tandem with 5G innovations.

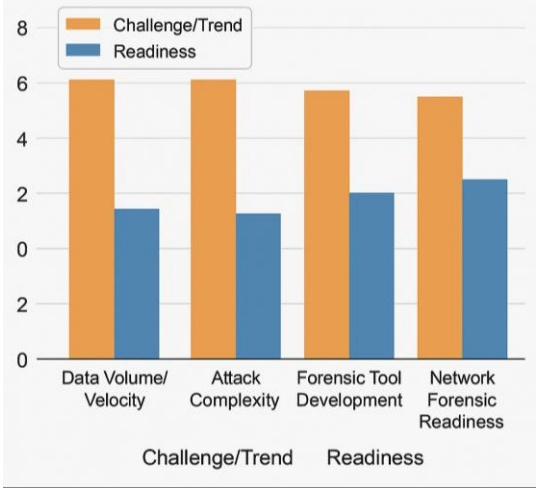

Fig.3 Digital Forensics in 5G Networks

CONCLUSION

Digital forensics in 5G networks presents both a transformative opportunity and a complex challenge. The shift toward decentralized architectures, edge computing, and network slicing demands a rethinking of traditional forensic techniques. While advancements in AI, virtualization, and real-time monitoring offer promising solutions, many forensic strategies remain in conceptual or developmental phases. Ensuring forensic readiness in 5G requires standardized logging, cross-layer visibility, and collaboration between network engineers, security experts, and legal authorities. As 5G continues to evolve, integrating digital forensics by design will be crucial to maintaining trust, accountability, and security in next-generation communication systems.

References

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2020). *Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.*

Zhang, Y., Wang, Y., & Lin, X. (2020). *Forensic-by-design for secure and privacy-preserving 5G network slicing. IEEE Network, 34(6), 100–106.*

Hassan, M. I., Rehman, A., & Anwar, Z. (2021). *AI-enabled forensic readiness for 5G-based smart infrastructures. Journal of Information Security and Applications, 58, 102744.*

ETSI (European Telecommunications Standards Institute). (2020).

ETSI GR NFV-SEC 012 V3.1.1 - Security; Network Functions Virtualisation (NFV); Security and Trust Guidance.

ITU-T (International Telecommunication Union - Telecommunication Standardization Sector). (2019). *Y.3056: Framework of network slice lifecycle management for IMT-2020.*

Sari, A., & Yildirim, S. (2019). *Digital Forensics in 5G Mobile Communication Systems: Challenges and Research Directions. Proceedings of the International Conference on Information Security and Cyber Forensics (InfoSec).*

Gauravaram, P., & Kumari, S. (2020). *Forensic logging and auditing in Software-Defined 5G networks.*

International Journal of Network Security & Its Applications (IJNSA), 12(4).

Ghosh, U., & Conti, M. (2019). *Privacy and Forensics Challenges in 5G Network Function Virtualization. IEEE Communications Magazine, 57(12), 86–92.*