Journal of Progress in Electronics and Communication Engineering, ISSN: 3048-7625 Vol. 3, No. 2, 2026 (pp. 76-84)
RESEARCH ARTICLE WWW.ECEJOURNAL.IN

Communication-Centric Security Models for Mobile Digital Learning Systems

Kesufekad Metachew[1], Letahun Nemeon[2], Dinfe Egash[3], Kasil Teyene[4]
[1-4]Electrical and Computer Engineering Addis Ababa University Addis Ababa, Ethiopia

KEYWORDS:
Security-aware communication algorithms,
Wireless network security,
Adaptive authentication,
secure handover management,
Quality of service (QoS),
Mobility-aware security,
End-to-end latency,
Packet delivery ratio

ARTICLE HISTORY:
Submitted : 26.12.2025
Revised : 16.03.2026
Accepted : 19.04.2026

https://doi.org/10.31838/ECE/03.02.11

Abstract

The fast penetration of mobile digital learning systems has further enhanced high dependency on the heterogeneous wireless communication network, which poses strong security issues pertaining mobility, dynamic nature of traffic and continuity of real-time sessions. Traditional security infrastructures are largely application-oriented, and take on a static form, which cannot be suitable in both latency sensitive and mobility-based learning environment. The paper suggests a communication-based security model of mobile digital learning systems, where the security enforcement is closely coupled with dynamics of the communication layer. An adaptive communication algorithm that is security-conscious is created to dynamically change the decisions of authentication, encryption and secure handover decisions in response to network conditions, mobility patterns and perceived threat levels. The suggested model is tested with the use of extensive simulation with different learner densities, mobility speeds and attack cases. The evaluation of performance is based on a set of security metrics comprising of authentication success rate, attack mitigation rate, and secure session establishment time, and communication metrics, such as end-to-end latency, throughput, and packet delivery ratio, and handover delay. The comparison of the results with the results of a static and rule-based security schemes proves that the proposed approach is significantly better in improving the communication reliability and security robustness, with low latency and manageable overhead. These results emphasise the power of the communication-based security model as a comparable and viable approach to secure mobile digital learning in upcoming wireless networks of the next generation.

Author's e-mail Id: metachew.kesu@aait.edu.et, nemeon.letahun@aait.edu.et, egash.din@aait.edu.et, teyene.kasil@aait.edu.et

How to cite this article: Metachew K, Nemeon L, Egash D, Teyene K. Communication-Centric Security Models for Mobile Digital Learning Systems, Journal of Progress in Electronics and Communication Engineering Vol. 3, No. 2, 2026 (pp. 76-84).

Introduction

Modern education has been transformed by the rapid growth of mobile digital learning systems as access to learning materials anytime and anywhere without restriction to heterogeneous wireless networks is now possible including Wi-Fi, cellular 5G, and edge-assisted communication information systems. The integration of mobile gadgets, cloud computing, and edge computing has dramatically enhanced the accessibility and scalability of learning opportunities, whereas it has also raised the risk of exposure to the security threats of all communication layers that have a direct effect on the reliability of services and the trust of the users.[1, 8, 10] Since mobile learners are often travelling between network domains, secure, low-latency, and continuous communication has been a core requirement of digital learning environments of the next generation. The dynamics introduced by mobility such as frequent handovers, changing network characteristics, and changing loads of traffic creates significant security risks such as unauthorised access, session hijacking, man-in-the-middle attacks, and replay attacks.[4, 7, 14] They are especially acute in edge-enabled systems where authentication, data processing and access control are shared among several areas of communication and network nodes.[8, 12] In these environments, the decoupled security mechanisms tend to create higher latency and unnecessary signalling overhead as well as poor quality of experience in learners.

The majority of the available security solutions to the mobile learning systems are application-centric based security solutions and are based on preset facilities of

authentication and pre-established policies of access control mechanism. Though these methods avail fundamental security assurances, they do not have the flexibility, to react to transient network alterations and mobility situations, and cannot be used to support large-scale as well as time-aware mobile-learning implementations.[5, 11] The latest studies on the topic of the zero trust architecture and adaptive security models have highlighted the element of constantly verifying and dynamically enforcing policies in wireless setup and edge setting; though, the actual implementation of these services alongside communication-layer decision making is not extensively promoted.[2, 3, 6, 9] This has been driven by the fact that communication based security modelling techniques are required where security mechanisms are tightly coupled with network states, mobility patterns and performance of communication requirements. This could be achieved by making the security information a direct part of the communication layer so that the security robustness, latency constraints and signalling overhead could be dynamically balanced which would result in security protection and efficient communication in any mobile learning environment.[3, 14]

Thus, the paper presents a security-conscious model of communication across the mobile digital learning systems that are functioning on the heterogeneous wireless networks. The scheme presented is a combination of adaptive security algorithms at the communication layer and can dynamically adapt authentication, protection as well as handover decisions based on the conditions observed in the network and mobility. The performance of the proposed model is corroborated by a comprehensive performance analysis that is based on security metrics of authentication success rate, secure session set up time, and communication metrics of end-to-end latency, throughput, and packet delivery ratio as well as handover delay. These findings prove the ability of the proposed communication-centric security model to immensely improve security resilience with minimal competition to efficient and reliable communication performance during mobile digital learning experience.

Related Work

Mobile digital learning systems security has been one of the research studies that have received more interest as educational service delivery has been expanding significantly over the use of wireless and mobile communication infrastructures. The initial research mainly concentrated on application-layer access control, user authentication and encrypted messages as clearance methods to secure learning resources and user data. Although they offer programmes to meet the basic security demands, in most cases, they operate under the assumption that the network connectivity and movement are stable and therefore do not insist in dynamic mobile learning applications where the mobility of learners is constantly changing through heterogeneous wireless networks.[11, 14] The current developments of wireless communication and mobile edge computing removed research priorities over communication-layer security especially in 5G- and edge-enabled networks. The 3GPP 5G security architecture standards focus on secure authentication, key management, and continuity of the sessions at communication layer to underpin mobility and low-latency based services.[1] Security issue and its mitigation strategies in the context of multi- party access edge computing environments have been studied complementarily, which illustrate weaknesses in areas of distributed authentication, handover operations, and inter-domain communication.[8, 10, 12] These papers highlight the significance of incorporating security measures in the communication processes to ensure reliability and performance in the presence of mobility.

Learning and adaptive security models have become promising to overcome the shortcomings of the old-fashioned security models. The idea of zero trust architecture supports constant verification and enforcement of policy in a dynamic way, so it is highly applicable in the dynamic wireless environment.[2, 3, 5, 11] Further extensions of zero trust concepts to 5G and 6G networks also apply machine learning solutions to improve threat detection and adjustment of policy in reaction to evolving conditions in the network.[6, 9] Simultaneously, security mechanisms such as learning-assisted security have been explored in regards to high and speedy handover authentication, especially in highly mobile networks like vehicular networks and edge-enabled networks.[4, 7] Such schemes exhibit better security strength and less authentication response times than traditional schemes.

Though these developments have been made, the current literature has a number of limitations. The vast majority of security solutions combine either application-layer security or communication security without special reference to real-time communication performance indicators, like throughput, latency and packet-delivery ratio. In addition to this, mobility-aware security adaptation is not considered as a design principle but more as an auxiliary aspect and this has led to poor functionality in cases where there is a frequent handover as well as variation in traffic. Figure 1, which suggests the deprivation of holistic models of communication-driven approaches that simultaneously address the aspects of mobility, adaptability, and performance

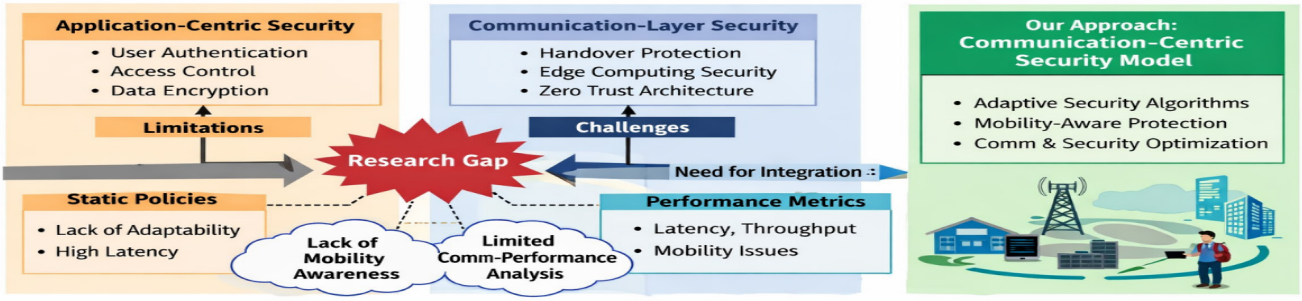

Fig.1: Conceptual taxonomy and research gaps of existing application-centric and communication-layer security models in mobile and edge-based communication systems.

on the communication level, illustrates a conceptual comparison of the existing solutions and limitations of the existing approaches and the positioning of the proposed work. In a nutshell, although the existing literature has formed a solid base in wireless security, edge computing and adaptive protection schemes, there still exists a gap in the research on the design of communication-specific security frameworks that are specifically applicable to mobile digital learning systems. To cope with this gap, support is needed in terms of security mechanisms that are intrinsically sensitive to parameters of communication and can adjust to the variations brought by mobility whilst ensuring high security levels.

System Model and Threat Assumptions

The system model which is taken into consideration in the present paper portrays a mobile digital learning environment which is using heterogeneous wireless communication networks as shown in Figure 2. It is made up of mobile learners, who have smart devices, wireless access points and base stations that provide access to different services, edge servers that are deployed near access network, and centralised learning platforms deployed on core network. Learning content, interactive sessions, and sharing of assessment data by Mobile learners are achieved with the help of these interconnected network components which, together, facilitate mobility, scalability and real-time provision of the services.

The system has a hierarchical flow of communication between the access, edge and core networking layers. The mobile learner devices at the access level form a wireless linkage with the access points or the cellular base stations, as a result of which the initiation of the session and the transmission of real-time data becomes possible. Latency-sensitive services such as content caching, session management and preliminary security enforcement are supported by the edge layer thus minimising end-to-end delay and enhancing service continuity when learners move between services. The central network contains central thus the learning management systems, policy control across the globe and long term data storage. Confidential communication sessions are ensured throughout network sections especially in handover instances, where continuity on authentication and a continuous manner is of prime concern in ensuring that there is no loss of service and no security leakage.

The threat model presumes the existence of attackers who can use the vulnerabilities that are presented by wireless communication and mobile environments. Passive eavesdropping attacks are also taken into consideration whereby the attackers intercept wireless communications to obtain confidential learning information or usernames. Active man in the middle attacks are also presumed allowing attackers to receipt, alter, or inject ill-intentioned packets on the communication sessions that are already underway. Furthermore, the illegal access attempts are also taken into consideration in the process of handover since in highly mobile settings, the process of re-authentication and managing keys quite often creates the probability of attacks.

The model also considers session hijacking and replay attacks in which the attackers can seek to use staling or loose security enforcement to access the learning services in an illegitimate manner. Attackers are expected to have enough computational and combative capability to track wireless channels, restate intercepted messages, and endeavour to make unauthorised session initiation cross networks boundaries. Nevertheless, they assume that cryptographic primitives are safe and trusted infrastructure, e.g. edge servers, or core learning platforms are physically undamaged. These assumptions make it possible to analyse the suggested communication-based security mechanisms in a realistic manner by working with dynamic and adversarial circumstances at the same time and by maintaining the practical nature of the system model.

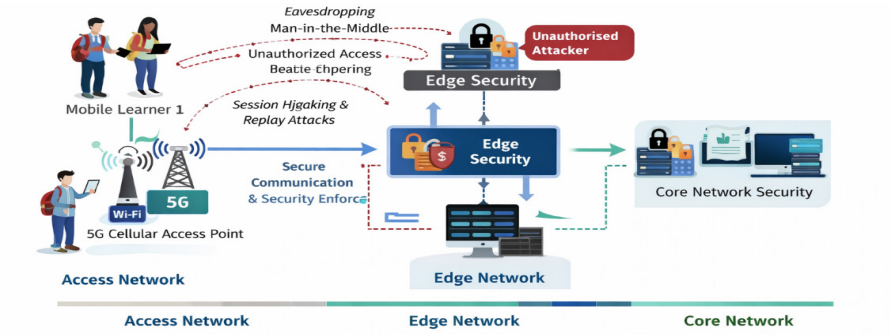

Fig.2: System architecture of the mobile digital learning environment with communication-centric security enforcement.

Communication-Centric Security Model

The communication-based security model suggested is meant to be fully embedded to link security functions with the operations of the communication layer in mobile digital learning systems, thus solving the shortcomings of stationary and application-driven protection plans. The model, as shown in Figure 3, inserts security enforcement throughout more than one layer of the communication stack in a modelled fashion, to provide coordinated and responsive protection to network conditions, mobility patterns, and performance requirements. At the physical level, the model presupposes baseline signal protection mechanisms that characterise contemporary wireless systems, which includes secure modulation, channel coding, interference resilience and so forth, which give a base level of confidentiality against passive eavesdropping. Although physical-layer security is not directly optimised in the given work, it creates trustful communication environment on the basis of which operations of higher-layers of the security can be performed with appropriate reliability. These assumptions enable the security model to concentrate on higher-level mechanisms of adaptive protection with attaining the basic nature of transmission integrity.

The model that will be used at the medium access control and network layers incorporates authentication, authorization, and routing security in the communication processes. They can use mobility-conscious authentication schemes to make sure that mobile learners can pass through access points and network domains safely without experiencing exorbitantly long re-authentication time. The routing and forwarding decisions are updated dynamically according to the state of the network and apparent level of threats to minimise exposure to attacks like session hijacking and unauthorised access during the handover events. The model will allow quick adaptation to changes caused by mobility without sacrificing communication efficiency due to the implementation of these security functions into the communication layer.

The model at the transport and application interface is concerned about the continuity of secure session regarding mobile digital learning services. Session management systems are developed to provide end-to-end confidentiality and integrity in content delivery and interactive learning processes and assessment exchanges. To reduce the replay and man-in-the-middle attacks, secure session identifiers and adaptive rekeying strategies are used especially when the level of mobility is high and the network conditions are not predictable. Such cross layer coordination has the benefit of ensuring that the security enforcement is similar at cross communication boundaries and service layers.

Three principles lead to the design of the communication-centric security model. First, the security enforcement with low latency is given top priority to avoid incurring quality of service deterioration of delay-sensitive learning applications. Second, the mobility sensitive authentication schemes will be used to ensure smooth movement of learners across heterogeneous wireless networks without undermining high security assurances. Third, adaptive control of security overhead is added to achieve a trade-off between the power of protection and communication services and, as such, the system dynamically adjusts the level of security accordingly with regard to real-time network conditions and threat analysis. All these principles put together, as shown in Figure 3, support a scalable and flexible system of security that improves both the reliability of communication and security strengths in the mobile digital learning setting.

Security-Aware Communication Algorithms

The proposed security-aware communication algorithm aims at maximising communication reliability and security robustness of mobile digital learning systems and reduces the end-to-end latency and security overhead minimization. There is a tendency to have inefficient use of resources or insufficient protection in highly dynamic wireless environment triggered by static security settings.

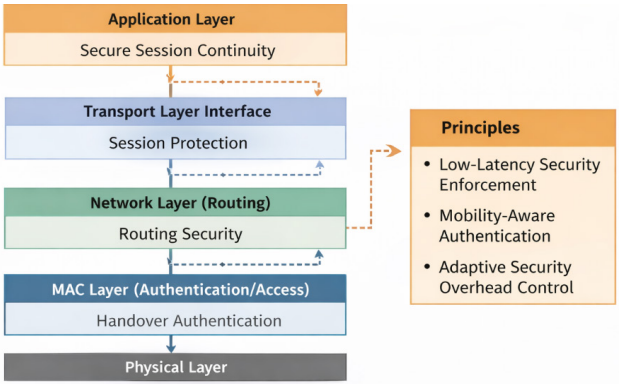

Fig.3: Layered communication-centric security model for mobile digital learning systems

The security decision-making problem is hence defined as a collaborative optimization problem that is balanced between the security strength and communicational performance in mobility-based circumstances. In this formulation, some clear constraints explored include the mobility of learners, the presence of limited wireless bandwidth and the energy limitations on mobile devices, which have an impact on the viability and performance of real-time security implementation.

To resolve this issue, an adaptive security-conscious communication algorithm is suggested because security settings are dynamically chosen depending on monitored network circumstances, mobility pattern, and perceived menace degree. The algorithm implements a learning-based or optimization-oriented approach that allows customization of the choice of security without adhering to any rigid policies or hard limits. Unnecessary signalling in case of a stable connexion while increased verification in case of a mobility event or an insufficient threat condition are accomplished by adjusting authentication frequency dynamically. In the same manner, the level of encryption is dynamically controlled to maintain the confidentiality and integrity without causing high computational complexity and energy usage. The algorithm is subjected to secure handover decisions to maintain the continuity of the sessions and prevent unauthorised access in the change between access points.

The algorithm works with a perception, decision action workflow. The system monitors the state information of the communication environment in an ongoing manner, which consists of network performance metrics like latency, the ratio of packet deliveries and bandwidth to get, and mobility metrics like handover rate and movement pattern of the user. The state representation also includes security-related signals, such as threat intensity, which is inferred or more broadly, the anomaly detection signals. On the basis of this contextual data, the algorithm makes the right security choices such as the choice of the security level, triggering re-authentication, changing the security encryption parameters, and activating secure handover. This is based on a reward or cost cost-function that collectively points to efficiency of communication and security effectiveness to advantage low latency, high reliability and successful mitigation of the attack whilst discouraging excessive overhead and security failure. Gradually, by reacting to the changing environment, the algorithm tends to the steady security policies which reach the desirable balance between the protection and performance.

To evaluate its performance, the proposed adaptive algorithm is evaluated against popular online schemes used. These encompass fixed security policies involving fixed authentication and encryption parameters, a rule based communication security mechanism, which is governed by predetermined heuristics and the standard authentication protocols prevalence in the wireless networks. These baselines can be characterised as representative points of reference concerning determining the advantages of adaptive and communication-oriented security decision making. The comparative analysis is aimed at the enhancements of communication reliability, latency minimization, efficiency of overheads, and robust security, which prove the efficiency of the proposed strategy in the mobile digital learning setting.

Performance Evaluation Methodology

The effectiveness of the proposed communication-focused security model and security-sensitive communication algorithm is measured with the help of comprehensive simulations in heterogeneous wireless networking environment mimicking mobile digital learning systems. The simulation model is based on an access network, edge computing infrastructure and centralised learning platform that simulates realistic communication and security interactions between access, edge, and core network segments. Wireless connexions are simulated with adjustable bandwidth, propagation delay and packet drop attributes to approximate reality of the network dynamics as well as to allow the representation of network latency sensitive learning services to be evaluated. The mobile learner devices produce learning related traffic, which is reflective of online digital learning activities such as delivery of content, interactive learning and evaluation data interactions. Periodic and bursty traffic are both taken to represent both the asynchronous access to learning and real-time communication needs. Modelling

of learner mobility involves the popular mobility models that emulate the user mobility in the covered areas of networks, and learners move between access points and base stations, leading to a high frequency of handover. It is a mobility modelling that provides the opportunity to systematically analyse the continuity of sessions, authentication behaviour, and system reliability in communication in dynamic conditions.

In order to test the security robustness, the simulation environment has several adversarial cases at the communication layer. Passive and active attacks strategies are modelled to examine the confidentiality and authentication and session management resiliency respectively. It is assumed that attackers will be able to trace wireless channels and inject or re-use packets without affecting trusted infrastructure elements. This modelling of threats allows realistic analysis of performance under security in benign and adversarial conditions. The assessment is conducted to look at various operational scenarios in order to control the behaviour of the system under different workloads and intensities of mobility. The population of concurrent mobile learners is also mixed to investigate scalability and its influence on communication performance levels, security overheads, and authentication success. Variations in speed of mobility are also taken to reflect stationary user, pedestrian mobility and high-mobility users and to be able to measure handover effectiveness and security adaptation to mobility. Besides, a performance is measured in both normal mode and attack mode so as to measure the trade-offs between communication efficiency and security robustness. All these evaluation scenarios offer a holistic evaluation of the suggested approach and portray it as effective in providing secure, reliable as well as low-latency mobile digital learning services.

Security and Communication Performance Metrics

In order to fully assess the applicability of the suggested model of communication-based security, a performance metric set is established to model the security resilience, communications efficiency, and system overhead in m-digital learning. These metrics are chosen to capture the efficacy in protection to adverse conditions, as well as quality-of-service needs with respect to learning matters that are sensitive to latency. Security performance is evaluated based on the metrics that measure the capacity of the system to thwart, identify, and reduce attacks without disturbing trusted access to the system by authorised users. Authentication success rate is the ratio of the number of valid attempts to authenticate that actually happen and form a measure of how secure the enforcement of security applies in the course of normal operation and mobility incidents. The rate of attack detection and mitigation assesses the system advertisement in the detection and mitigation of malicious actions like replay, man-in-the-middle, and session hijacking attacks. To handle the inaccurate security decisions, the false positive rate is taken into consideration that would measure the number of times legitimate users or sessions are mistakenly identified as a malicious user. Moreover, secure session establishment time is also an aspect that is estimated to determine the amount of time wasted in establishing or re-establishing secured communication sessions especially during handovers and dynamic network states.

The communication performance is measured by the metrics that directly affect the user experience and continuity of the service of mobile digital learning systems. End-to-end latency is an indicator that summarises the total delay incurred by learning data packets, transmitted by the mobile learner, to the learning platform, which includes the delay associated with transmission, processing, and delay associated with security concerns. Throughput measures the effective data rate of the system, which shows the capability of delivering large amount of learning contents and interactive classes. Packet delivery ratio is an evaluation that helps towards measurement of communication reliability by the relative number of packets delivered as compared to the number of packets that are sent. As a critical measure of the mobile environment, handover delay measures how long it takes to change the active learning sessions between the access points or base stations without interrupting the service. Besides performance in terms of security and communication, system overhead measures are utilised to measure the cost of security enforcement. Security signalings overhead is used to assess the control traffic added due to the authentication, key management processes and security coordination processes. Computational delay Model captures the processing time of activities associated with security like encryption, decryption, and cryptography which will be directly related to the latency and responsiveness of a security device. The measurement of the consumed energy per session is taken to evaluate how adaptive security mechanisms affect the battery life of mobile learner devices, which is a crucial factor in the sustained learning activities.

Combined with each other, these metrics can allow evaluating the proposed approach holistically and understanding the trade-offs between the strength of the security, communication effectiveness, and utilisation of

resources. Through the combined nature of assessment of security effectiveness, communication performance, and overhead the evaluation framework offers an employable framework to assessing the appropriateness of communication-centric security modelling of mobile digital learning systems.

Results and Discussion

In this section, a thorough comparison of the proposed communication-centric security model with that of input baseline schemes include: static security policy, rule-based communication security as well as traditional authentication scheme is provided. The summary of the comparative results as represented in Table I indicate that the proposed adaptive approach has a consistent outperformance over the base schemes in terms of security and communication performance measures. Specifically, much more authentication success rates and a more effective attack mitigation capability are obtained, without requiring excessive overhead of communicating with the security decisions directly, which signify the benefits of the integration of security decisions with the dynamics of the communication layer. The evaluation is influenced by the adaptive security implementation on the time of communication. As Figure 4 illustrates, the proposed model achieves much lower end to end latency than the baseline schemes as network load and mobility intensity increase. The adaptive algorithm unlike the static and rule-based security tools cause significant delays, since they often require a re-authentication and inflexible security settings but in practise, the adaptive algorithm dynamically increases or decreases the frequency of authentication and the security level based on real-time conditions. This provides less signalling overhead and quicker session setup, that are vital to delay-sensitive mobile digital learning services.

The effectiveness of the presented model is further discussed with the help of the trade-off between the strength of the security and the overhead of the system. The findings have shown that adaptive control of security parameters can allow the security system to implement a stronger security during the periods of high risk and loosen the security enforcement in times of stable conditions. This is an adaptive behaviour in that there is a balanced trade-off where strong security is obtained at the moderate cost of computational and signalling costs. Conversely, baseline schemes either manage to maintain high overhead at all times because of the overprotected security settings or expose the system to attacks because they prioritise performance over security. The results prove that communication-oriented security modelling allows to better use the resources of networks and devices.

The resilience of the established solution is also checked in terms of its high mobility and attack intensity that is to justify the robustness of the channel. The proposed model provides high ratios of packets delivery and reduced handover delays with high security guarantees within a situation where the percentage of handovers is high and the aggression rate of attacks is elevated. Adaptive security-aware communication algorithm can prevent profuse session hijacking, replay and man in the middle attacks by forcibly strengthening authentication, and session protection mechanisms when an individual undergoes mobility. Baseline schemes on the contrary show poor performance and heightened authentication failure in similar conditions. All these findings attest to the suggestion that the communication-based securitv model offers a viable and secure solution to

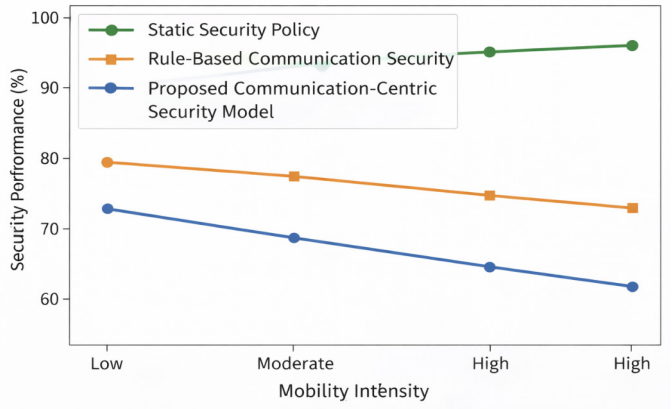

Fig. 4:. Security performance versus mobility intensity under attack conditions.

Table 1: Security Performance Comparison of Different Communication Security Schemes

Security Scheme	Authentication Success Rate (%)	Attack Mitigation Rate (%)	False Positive Rate (%)	Secure Session Establishment Time (ms)
Static Security Policy	91.4	86.2	7.8	185
Rule-Based Communication Security	94.7	90.5	5.3	142
Proposed Communication-Centric Security Model	**98.3**	**96.8**	**2.1**	**88**

the secure digital learning systems that are based on mobile and work in dynamic and adversarial wireless environments.

Practical Implications

The proposed security model based on communication has multiple practical implications on the implementation and implementation of practical mobile digital learning platforms. With the model, whose implementation is based on the direct combination of security enforcement with communication-layer processes, it can be easily implemented within present-day mobile learning systems that are based on the use of heterogeneous wireless networks. The security-aware communication algorithm is adaptive to enable learning services to be sustainably and reliably connected in changing mobility and traffic conditions, and is therefore suitable in the large-scale deployment in smart campuses, public learning environments and remote education platforms.

The compatibility with the existing wireless standards is one of the strengths of the proposed solution. This security model is compatible with standard communication and security models in modern wireless networks, such as 5G and edge computing models, due to the usage of well-known authentication and session management principles and handover processes. The proposed model does not substitute the current protocols, but it improves them by bending them to more intelligent decisions in response to situational conditions at the communication layer. The design enables the existing network infrastructures to be integrated without major adjustments to the underlying hardware or protocol stack which eases deployment.

The proposed approach has practical benefits in various functions within the mobile learning ecosystem as seen through the perspective of the stakeholders. The learners enjoy better service continuity with less latency as well as protection of personal and learning data despite the unfavourable network-conducted latency and high mobility. It also gives educators more trustworthy and safe places that facilitate interactive and real-time learning processes without interference. Adaptive security management is beneficial in networks in which system administrators and network operators need less manual-configurator resources and capabilities to increase resource utilisation and resilience against emerging security threats. All these practical benefits go to show the viability and worth of communication based security modelling in achieving secure, scalable and efficient mobile based digital learning systems.

Limitations and Future Work

Although the suggested communication-based security model is promising in terms of its performance in mitigating the security of mobile digital learning systems, its performance should be limited in the following aspects. Evaluation given in this paper relies on simulation experiments and these experiments, though effective at controlled and repeatable experimentation, may not be able to be representative of all the dynamic behaviour of a network and behaviour of users in real life. The performance of such a system can be affected in a practical deployment due to things like unpredictable interference on wireless connexions, heterogeneous capabilities of devices, and interaction by mass users that are hard to model holistically in a simulation system. There are also some assumptions incorporated in the threat model used in this paper which can potentially act as a constraint to the generality of the findings. Attackers will be expected to use the communication level without tampering with trusted infrastructure elements including edge servers or core learning platforms. Although this assumption represents most realistic attack scenarios, more advanced attackers that also can conduct insider attacks or a multi-vector attack might be an even stronger challenge. Such capabilities of the adversary would be worth extending the threat model to give a more comprehensive evaluation of the security framework.

These limitations can be mitigated by future research by implementing the proposed approach in a number of ways. The role of multi-agent security coordination can be studied to facilitate joint security decision making among distributed network entities to enhance scalability and responsiveness in large scale mobile learning system. Another potentially promising direction is provided by edge cloud collaborative security solutions, where security-related knowledge is exchanged between edge nodals and centralised information systems to enhance global awareness and threat mitigation. Moreover, the combination of security measures with learning analytics might facilitate context-based protection measures altering based on the network conditions as well as learning behaviours and patterns of usage. Such extensions in the future would provide additional flexibility, strength, and functionality to the communication-related security models in the next generation of mobile digital learning systems.

Conclusion

The given paper has introduced a model of the security of mobile digital learning systems where

security enforcement is closely connected with the communication-layer dynamics to consider the issues posed by mobility, a heterogeneous wireless network, and the changing security threats. The proposed system achieves the balanced security, communication reliability and the performance efficiency challenges by integrating adaptive security mechanisms throughout the communication stack and using security-aware communication algorithms. The evaluation using simulation indicated that the adaptive algorithms provide significant enhancement of authentication reliability, ability to mitigate the attack and maintain the session continuity, low latency as well as manageable overhead in face of different mobility and attack conditions. The findings also provide the significance of communication-focused security modelling as a realistic and scalable tool to facilitate secure, reliable, and high-quality mobile digital learning services in next-generation wireless settings.

References

[1] 3GPP, B. (2020). Security architecture and procedures for 5G system. *Technical Specification (TS) 3GPP TS 33.501 V17. 0.0 (2020-2012)*.

[2] Alnaim, A. K. (2025). Adaptive Zero Trust Policy Management Framework in 5G Networks. *Mathematics*, *13*(9), 1501.

[3] Chen, X., Feng, W., Ge, N., & Zhang, Y. (2023). Zero trust architecture for 6G security. *IEEE network*, *38*(4), 224-232.

[4] Goswami, B., & Choudhury, H. (2024). A secure and fast handover authentication scheme for 5g-enabled iot using blockchain technology. *Wireless Personal Communications*, *138*(4), 2155-2181.

[5] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1), 6476274.

[6] Ishihara, A. K., Abdelbaky, M., & Shetye, S. (2023, January). Zero-Trust Architecture for Autonomous Edge Computing. In *Scitech 2023*.

[7] Krishnan, P., Jain, K., Alluhaidan, A. S. D., & Prabu, P. (2024). Highly secured authentication and fast handover scheme for mobility management in 5G vehicular networks. *Computers and Electrical Engineering*, *116*, 109152.

[8] Nencioni, G., Garroppo, R. G., & Olimid, R. F. (2023). 5G multi-access edge computing: A survey on security, dependability, and performance. *IEEE Access*, *11*, 63496-63533.

[9] Ramezanpour, K., & Jagannath, J. (2021). Intelligent zero trust architecture for 5g/6g networks: Principles. *Challenges, and the Role of Machine Learning in the context of O-RAN. arXiv*.

[10] Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on multi-access edge computing security and privacy. *IEEE Communications Surveys & Tutorials*, *23*(2), 1078-1124.

[11] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 1-52.

[12] Shafee, A., Awaad, T. A., & Moro, A. (2024, July). A Survey of Edge Computing Privacy and Security Threats and Their Countermeasures. In *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (pp. 484-489). IEEE.

[13] Tochukwu, I. C., Nonyelum, O. F., Misra, S., & Chockalingam, S. (2025). Securing mobile edge computing: A survey on cyber-physical threat mitigation for digital sovereignty. *Procedia Computer Science*, *254*, 211-220.

[14] Wang, C., Yuan, Z., Zhou, P., Xu, Z., Li, R., & Wu, D. O. (2023). The security and privacy of mobile-edge computing: An artificial intelligence perspective. *IEEE Internet of Things Journal*, *10*(24), 22008-22032.