Authentication Handover and Privacy Protection in 5G HetNets Using Software-Defined Networking

Xiaoyu Duan and Xianbin Wang

The authors are with Western University.

ABSTRACT

Recently, densified small cell deployment with overlay coverage through coexisting heterogeneous networks has emerged as a viable solution for 5G mobile networks. However, this multi-tier architecture along with stringent latency requirements in 5G brings new challenges in security provisioning due to the potential frequent handovers and authentications in 5G small cells and HetNets. In this article, we review related studies and introduce SDN into 5G as a platform to enable efficient authentication handover and privacy protection. Our objective is to simplify authentication handover by global management of 5G HetNets through sharing of user-dependent security context information among related access points. We demonstrate that SDN-enabled security solutions are highly efficient through its centralized control capability, which is essential for delay-constrained 5G communications.

INTRODUCTION

Over the past few years, anywhere, anytime wireless connectivity has gradually become a reality and has resulted in remarkably increased mobile traffic. Mobile data traffic from prevailing smart terminals, multimedia-intensive social applications, video streaming, and cloud services is predicted to grow at a compound annual growth rate of 61 percent before 2018, and is expected to outgrow the capabilities of the current fourth generation (4G) and Long Term Evolution (LTE) infrastructure by 2020 [1]. This explosive growth of data traffic and shortage of spectrum have necessitated intensive research and development efforts on 5G mobile networks. However, the relatively narrow usable frequency bands between several hundred megahertz and a few gigahertz have been almost fully occupied by a variety of licensed or unlicensed networks, including 2G, 3G, LTE, LTE-Advanced (LTE-A), and Wi-Fi. Although dynamic spectrum allocation could provide some improvement, the only way to find enough new bandwidth for 5G is to explore idle spectrum in the millimeter-wave range of 30~300 GHz [2].

NETWORK ARCHITECTURE OF 5G

Due to the poor signal propagation characteristics at extremely high frequencies, future 5G networks will be heterogeneous with small cell deployment and overlay coverage, as shown in Fig. 1. Cellular networks operating at low frequencies (e.g., 2G, 3G, LTE, LTE-A) could provide wide area coverage, mobility support, and control, while small cells operating at higher frequencies guarantee high data rates in the area of spectral and energy efficiency.

This heterogeneous paradigm with multi-tier coverage in 5G not only follows the natural evolution from existing cellular technologies, but also satisfies the requirements of increased data traffic, with small cells providing very high throughput and underlying macrocells providing extensive coverage. Therefore, network densification using low-power small cells is widely considered to be a critical element toward low-cost high-capacity 5G communications.

SECURITY CHALLENGES IN 5G

Along with the advantages of 5G architecture in Fig. 1, there also come several major technical challenges. The massive deployment of small cells poses potential challenges in network management, including interference alignment, extensive backhauling, and inconsistent security mechanisms over heterogeneous networks (HetNets). Network management and service provisioning are challenging in this multi-tier model due to the increased number of base stations and complexity of network architecture. Therefore, new technologies are needed to provide intelligent control over HetNets for consistent and effective resource allocation as well as security management.

Moreover, 5G users may leave one cell and join another more frequently with reduced cell size, which could introduce excessive handover-induced latency in 5G. Future 5G applications like interactive gaming and tele-operations require 5G latency to be an order of magnitude smaller than 4G, with 1 ms target round-trip time [2]. However, due to smaller cell deployment, users and different access points (APs) in 5G need to perform more frequent mutual authentications than in 4G to prevent impersonation and man-in-the-middle (MitM) attacks. On the other hand, the power and resource constraints of small cell APs require low complexity and highly efficient handover authentication procedures. Therefore, faster, efficient, and robust handover authentication and privacy protection schemes need to be developed for complex 5G HetNets.

The Scope of This Article

In this article, we first introduce the 5G background and identify the challenges in 5G HetNets, especially in security management. Existing related studies are overviewed, providing a summary of the previous security solutions and state-of-the-art related technologies. Based on our survey and analysis, we believe that new solutions meeting the latency and complexity requirements of 5G HetNet communications are yet to be developed.

Based on this observation, we introduce a new 5G network structure enabled by software-defined networking (SDN) to bring intelligence and programmability into 5G networks for efficient security management. With SDN, the control logic is removed from the underlying infrastructures to a controller in the control layer [3] so that software can be implemented on the central SDN controller to provide consistent and efficient management over the whole 5G HetNet. With this paradigm, we propose an SDN-enabled user-specific secure context information transfer for efficient authentication handover and privacy protection in 5G to achieve seamless authentication during frequent handovers, while at the same time meeting the privacy and latency requirements effectively.

State of the Art in Handover Authentication and Challenges in 5G

Related Work on Handover Authentication and 5G Challenges

To support increased data traffic, 5G networks need to have high capacity and efficient security provisioning mechanisms. Densification of heterogeneous networks and massive deployment of small base stations become the natural choice for 5G. On the other hand, many applications supported by 5G, such as mobile banking and cloud-based social applications, require higher data confidentiality and reliable authentication against malicious attacks.

The common practice for secure communications in 3G and later wireless networks is based on admission control and cryptographic exchange. Figure 2 gives an overview of the handover authentication procedures between different networks and within one network [9]. The involved network components here are the user equipment (UE), access points (APs) or base stations (BSs), and an authentication server. It can be seen from Fig. 2 that mutual authentication during handover between the user and a new network (i.e., procedure 1) is realized by the pairing of specific hashing output. Each time the involved vector includes RAND, a random number known by the server, AUTH, an authentication token sent by the server, a pairwise key, and so on. For mobility within the same network (i.e., procedure 2), the current serving AP will inform the target AP of the possible handover so that the latter can retrieve the user authentication and key context from the server. In the following, we analyze existing handover authentication procedures and identify the challenges in 5G HetNets based on Fig. 2.

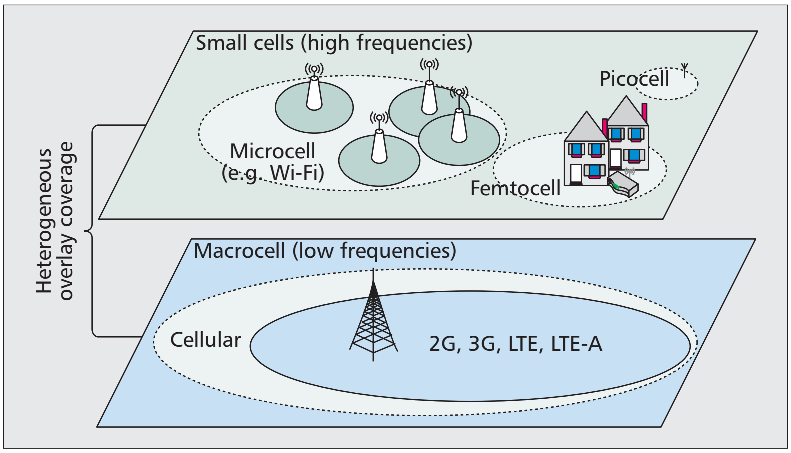
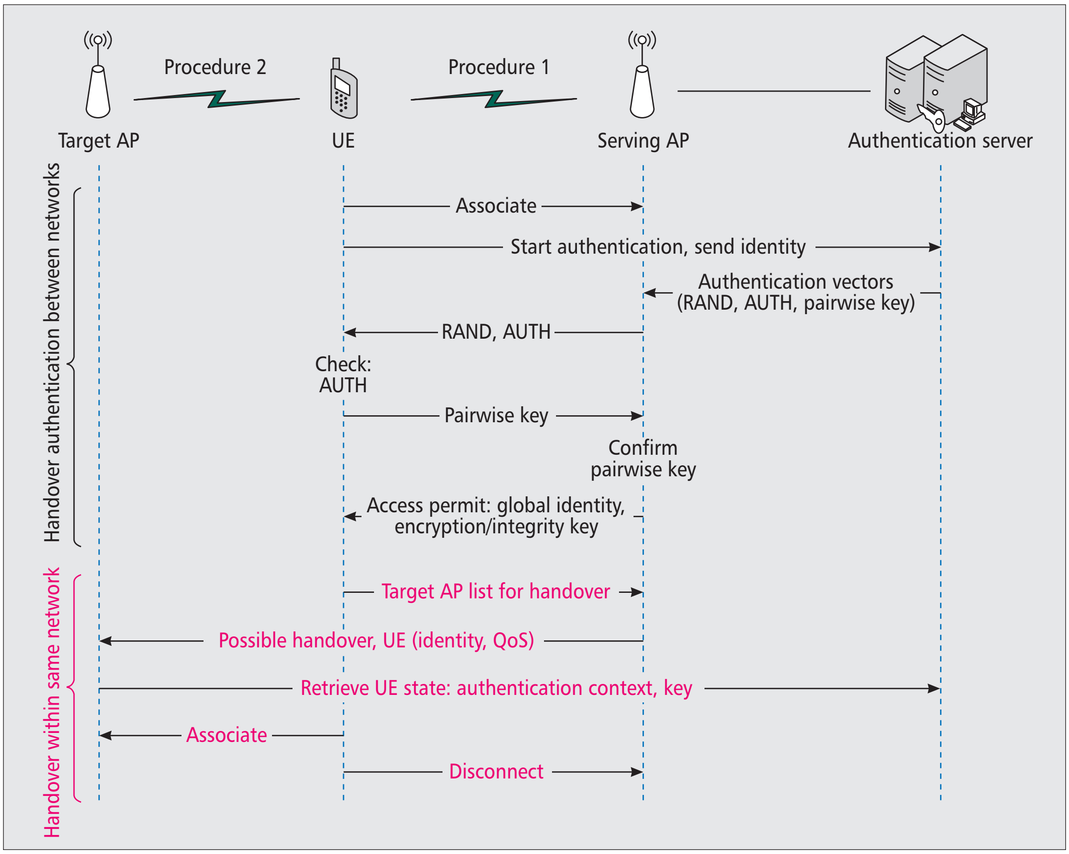

Small cells (high frequencies)
Picocell
Microcell
(e.g. Wi-Fi)
Femtocell
Heterogeneous overlay coverage
Macrocell (low frequencies)
Cellular
2G, 3G, LTE, LTE-A

Figure 1. 5G heterogeneous network structure with densified small cells and overlay coverage.

To enable handover between different wireless networks (i.e., procedure 1 in Fig. 2), various authentication servers and protocols are involved due to the closed nature and structure of each network in a HetNet, rendering frequent establishments of trust relationships and authentications during mobility, especially in a 5G small cell scenario [2]. The Third Generation Partnership Project (3GPP) has provided specific key hierarchy and handover message flows for various mobility scenarios [10]. However, the specific key designed for handover and different handover procedures for various scenarios will increase handover complexity when applied to 5G HetNets. As the authentication server is often located remotely, the delay due to frequent enquiries between small cell APs and the authentication server for user verification may be up to hundreds of milliseconds [5], which is unacceptable for 5G communications. The authors of [6, 7] have proposed simplified handover authentication schemes involving direct authentication between UE and APs based on public cryptography. These schemes realize mutual authentication and key agreements with new networks through a three-way handshake without contacting any third party, like an authentication, authorization, and accounting (AAA) server. Although the handover authentication procedure is simplified, computation cost and delay are increased due to the overhead for exchanging more cryptographic messages through a wireless interface [5]. For the same reason, carrying a digital signature is secure but not efficient for dynamic 5G wireless communications.

For handover within the same network (i.e., procedure 2 in Fig. 2), existing security mechanisms utilize complex context transfer, and it has

When introducing SDN into 5G networks, the SDN controller will have global control over the network, while SDN switches simply follow data forwarding instructions from the controller. Applications are implemented on top of the controller to define the behavior of the switches and APs, thus creating a reconfigurable 5G HetNet.



Procedure 2
Procedure 1
Target AP
UE
Serving AP
Authentication server
Handover authentication between networks
Associate
Start authentication, send identity
Authentication vectors (RAND, AUTH, pairwise key)
RAND, AUTH
Check: AUTH
Pairwise key
Confirm pairwise key
Access permit: global identity, encryption/integrity key
Handover within same network
Target AP list for handover
Possible handover, UE (identity, QoS)
Retrieve UE state: authentication context, key
Associate
Disconnect

Figure 2. Authentication processes of handover procedure 1, between different networks, and handover procedure 2, within the same network.

been found that most of the handover latency is due to the scanning time for identifying the target AP and round-trip time to the authentication server. Related work in [8] proposed a user-assisted authentication context transfer scheme, by which the current AP transfers a signed authentication certificate as a security context to the user, and then to the target AP through the user. The UE is actively involved in handover authentication with its existing connections with the current and next target APs to reduce latency. However, mutual trust between APs is assumed in these solutions, which could be infeasible for 5G HetNets due to the lack of direct interfaces between different networks. In addition, the transferred security context, which is just a combination of identity and signature, may not be secure enough to prevent 5G wireless communication from potential attacks.

In light of these challenges, robust and efficient handover authentication and secure context information transfer is crucial in securing 5G networks. The unique link characteristics experienced by each UE can be explored as a security context to accelerate authentication handover. Such user-specific attributes include physical layer attributes (clock skew, signal strength, channel state information), location, and even moving speed and direction [11], some of which have already been reported to APs for the purpose of resource allocation and seamless handover. It is believed that by taking advantage of these unique attribute combinations as non-cryptographic solutions, authentication can be faster, more robust, and less complex compared to widely used cryptographic exchange mechanisms [12].

Software-Defined-Networking-Enabled 5G Networks

Software-defined networking [3] is considered as a radical new network structure to centralize network management, and enable innovation through network programmability in meeting the needs of emerging applications. One main feature of SDN is decoupling the control plane and data plane by taking control logic from the underlying switches and routers to the centralized SDN controller in the control plane.

When introducing SDN into 5G networks, the SDN controller will have global control over the network, while SDN switches will simply follow data forwarding instructions from the controller. Applications are implemented on top of the controller to define the behavior of the switches and APs, thus creating a reconfigurable 5G HetNet, as shown in Fig. 3. The separation of data forwarding switches and the control plane enables easier implementation of new protocol and functions, consistent network policy, as well as straightforward network management.

In supporting SDN-enabled 5G, appropriate SDN protocols, such as Openflow and Simple Network Management Protocol (SNMP), will be added to base stations, access points, and wireless switches through an external standardized application programming interface (API) [4].

Importantly, OpenFlow is in charge of data path control, and SNMP can be used for device control. As the SDN controller is just a program running on a server, it can be placed anywhere in the 5G network — even in a remote data center.

An SDN-based 5G network structure enables flexible ubiquitous connection, fast rerouting, and real-time network management with the software controller. Users are able to access network services anywhere and anytime regardless of the network type [4] (e.g., Wi-Fi, 3G, LTE, LTE-A) as long as these networks belong to the same operator or there are agreements between operators. Furthermore, consistent authentication and privacy protection are also manageable.

In this article, we explore SDN as a promising platform to introduce intelligence into 5G and address the security challenges. Specifically, we discuss SDN-enabled authentication handover, which provides control over HetNet infrastructures and helps the network to reduce redundant authentications across HetNets. Handover authentication thus becomes a more controlled and prepared process instead of multiple independent procedures. By sharing secure context information along moving direction of the user and choosing multiple network paths to transmit data concurrently, the SDN structure is capable of facilitating 5G security provisioning more efficiently. In doing so, user-specific attributes are utilized as the shared security context to reduce handover complexity. To further achieve privacy protection, SDN-enabled data transmission over different network paths in 5G HetNets is also investigated in order to guarantee privacy.

SDN-Enabled 5G Authentication Handover

In this section, we introduce SDN into 5G to enable the proposed authentication handover scheme in coping with the frequent handover authentication in small cells and HetNets, as shown in Fig. 4. We implement an authentication handover module (AHM) in the SDN controller to monitor and predict the location of users, and then prepare the relevant cells before the user arrives to guarantee seamless handover authentication. Using a traffic flow template (TFT) filter [13] (source/destination IP addresses and port numbers) and related quality of service (QoS) description, secure context information (SCI) is collected by the AHM to share along a projected user moving path (i.e., from cell A to cell B, C in Fig. 4). The relevant cell APs thus prepare resource in advance and ensure seamless user experience during mobility.

Specifically, user specific attributes including identity, location, direction, round-trip time (RTT), and physical layer characteristics have been considered as reliable SCI to assist secure handover in 5G networks, instead of using complex cryptographic exchange mechanisms. As a non-cryptographic method, user-specific attributes are able to simplify the authentication procedure by providing the unique fingerprint of the specific device without additional hardware and computation cost [12]. In this article, we focus on using user-specific attributes as SCI (location, direction, etc.) to realize SDN-enabled authentication handover. Based on the proposed authentication context handover, security in SDN-enabled 5G networks becomes a monitored seamless procedure instead of multiple independent verifications, which could significantly reduce the possibility of impersonation and MitM attacks.

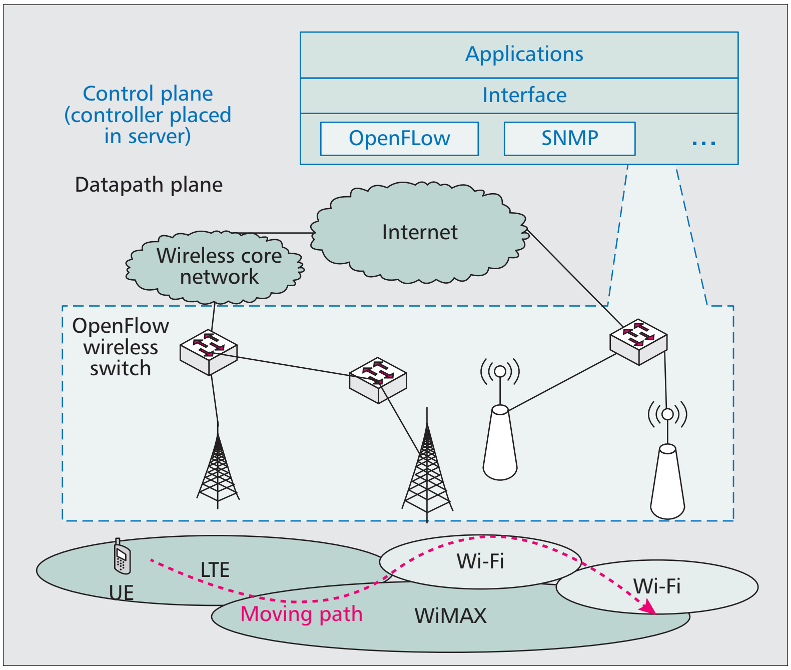


Figure 3. SDN-enabled 5G wireless HetNet structure with control plane design.

More precisely, the way in which the SDN controller shares the user's SCI to next cell APs along the predicted path is just like a trustworthy introduction from a previous AP before handover. The future cell APs thus finish authentication with the user quickly and begin to monitor the user to prepare service according to the SCI. As the trace of the user is monitored, the risk of impersonation is significantly, if not entirely, reduced. More importantly, there would be risk of service disruption in previous networks if the connection between APs and the authentication server is broken. Under similar network conditions, however, our mechanism will not lose global network connectivity because a new AP is monitoring the user, which can help the controller retrieve the necessary information according to the pre-shared SCI. Thus, the SDN-enabled security handover possesses high levels of tolerance to network failures. In the following, a description of the authentication handover mechanism in terms of assumptions and designs is presented in detail.

Assumptions and Design Goals

We assume that the SDN controller is a program running in a mobile operator's data center with an AHM for user authorization. The AHM is in charge of both authentication and handover, which maintains user information specifying what the user can access. The AHM also pos-

Due to the reduced cell size in 5G HetNets, users might move through multiple small cells before completing one communication session. Thus, the privacy protection is more challenging in 5G due to the possible involvement of untrusted or compromised APs during handover.

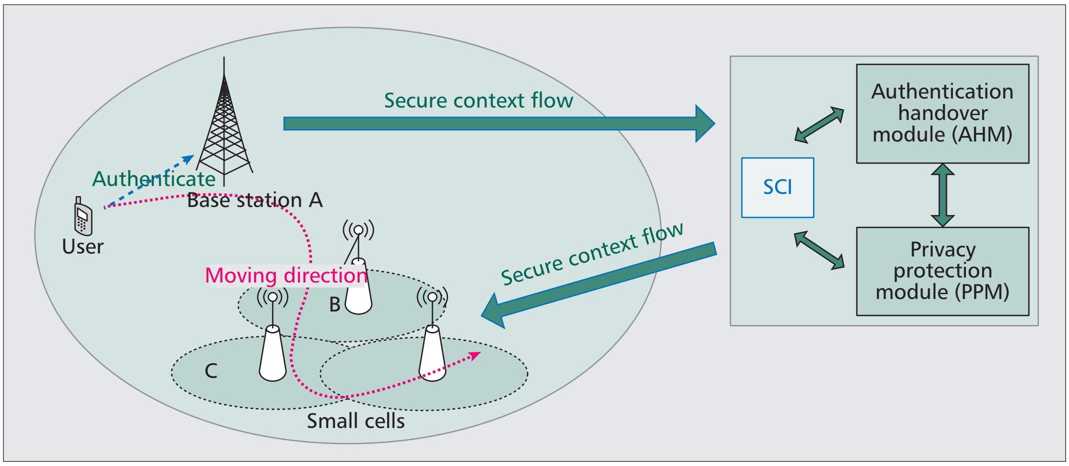


Figure 4. SDN enabled secure context information transfer between 5G UE, APs and AHM in SDN controller.

sesses a master public-private key pair (K, K^{-1}), with a public key K that is known to users and APs. Both APs and UEs need to be verified before gaining access to network services to reduce security risks.

Our design goal for the authentication handover mechanism is to accelerate authentication in 5G HetNets by enabling SCI transfer using SDN. In further reducing the overall authentication delay, the AHM in the controller could periodically authenticate the APs in off-peak times using its master key to avoid leakage of privacy caused by compromised APs. If certified, a key pair (K_N, K_N^{-1}) with a signature $[K_N, T]_{K-1}$ is distributed to the AP, where T is the timeout of the signature; if the AP is detected as compromised, it will be blacked out from further operation. This way, some of the authentication procedures are moved to off-peak times and relieves the SDN controller burden.

SDN-Enabled Authentication Handover Mechanism Design

With the assumptions and design goals described above, we can design the SDN-enabled authentication handover mechanism. User-specific SCI, such as ID, physical layer attributes, location, speed, and direction, can be collected and shared easily with SDN flow-based forwarding [3]. According to the UE location information from SCI, the SDN controller uses an ascending index to indicate the sequential order of next cells in the moving direction. Once authenticated by one cell AP, an appropriate combination of user attributes is then shared as SCI by the SDN controller along this user's future path. This way, the UE is able to enjoy seamless service without complex operation during authentication handover, thus saving time for data communications.

For example, we assume that user U is in cell A, and the future cells are B and C, as shown in Fig. 4. The authentication procedure between user U and cell A follows the commonly used authentication protocol [10], and the proposed SDN-enabled authentication handover procedure is described in Algorithm 1.

The SCI attributes in the proposed SDN-enabled authentication handover could include identity, physical layer attributes, location, moving speed, and direction. The number of attributes to be used is based on the security level of the information requested. For example, if the user is requesting banking or email services, a higher security level can be achieved by transferring more SCI attributes; if it is just Internet browsing or video gaming, the security level can be lower, and few SCI attributes are needed.

The aforementioned authentication handover method requires no changes to the existing UE and AP hardware, and significantly simplifies the authentication procedure and reduces handover latency through a non-cryptographic technique. By predicting the user moving path and shifting the authentication of APs to off-peak times, the SDN-enabled 5G networks can always be well prepared for other service requests. Moreover, operators can choose to switch off/on lightly loaded cells if the users approaching these cells are not going to exceed a certain threshold according to the SCI information to save more energy.

SDN-Enabled 5G Privacy Protection

Data privacy means the right of network users to seclude themselves from prying and eavesdropping. Due to the reduced cell size in 5G HetNets, users might move through multiple small cells before completing one communication session. Thus, the privacy protection is more challenging in 5G due to the possible involvement of untrusted or compromised APs during handover. Existing privacy protection schemes use complex key agreements and interactions or additional watermarking to protect data privacy. Such cryptographic methods bring computation burden and complexity to both the AP and client sides [9], which is undesirable for 5G low-power small cell infrastructures. On the other hand, privacy protection requires that no link can be established

State(A, U): Authenticated.
State(B, U): Not Authenticated.
State(C, U): Not Authenticated.
AHM → B: (*index* = 1, *ID*, *SCI*)
AHM → C: (*index* = 2, *ID*, *SCI*)
Ascending index number shows the direction of user movement. ID is the identity of *U* and *SCI* is the secure context information of *U*.
B → A: Handoff REQ(*ID*, *SCI*).
When *B* discovers *U* in its coverage, *B* sends handoff request to *A* until receives reply from *A*.
A → B: Handoff ACK(*ID*, *SCI′*).
A replies with handoff acknowledgement. *SCI′* is the secure context information which is more recent than previous shared *SCI*.
B → U: Update REQ().
After matching *SCI′* from *A* with *U*, *B* authenticates *U* and starts to associate with *U*.
U → B: Update ACK(*SCI″*).
Here *U* is connected with *B*. *SCI″* is the latest secure context information.
State(B,U): Authenticated.
B → AHM: Update(*SCI″*).
B updates the UE secure context information to AHM. AHM then shares secure information to next cell APs according to the location and direction information in new *SCI″*.
C → B: *C* keeps on monitoring *U* and follows similar procedure.

Algorithm 1. User-SCI-based authentication handover.

```
procedure PDO($n$)
    $T_S$: delay threshold
    $V_{sn} = b_n \min(t_r; T_S)$: size in bytes to be transferred in nearby Wi-Fi, Femtocell or cellular within $T_s$
    for $d_1 < V_{s1}, d_2 < V_{s2}, \ldots d_n < V_{sn}$ and $d = d_1 + d_2 + \ldots + d_n$ do
        Encrypt $d_1, d_2, \ldots d_n$ separately, send them on n networks concurrently and update $d$
    end for
    Receiver decrypt $d_1 \sim d_n$ using private key and re-organize data
end procedure
```

Algorithm 2. Partial data offloading over different SDN-controlled network paths.

between information and the owner, while authentication requires an identity provided for the purpose of authentication. Previously, these contradictory requirements were met through a trusted third party. However, multiple enquiries to the remote third party cause a network bottleneck, which is not suitable for 5G low-latency communications.

We introduce an SDN-enabled privacy protection scheme, which employs partial transmission over different SDN-controlled network paths to guarantee privacy and offload traffic in 5G cellular networks at the same time. With the proposed privacy protection scheme, SDN controller is able to choose multiple network paths to transmit different parts of the data stream (i.e., partial transmission) according to the HetNet coverage. The number of network paths is decided by the sensitivity level of the data stream. As long as the UE has been authenticated and is covered by the HetNets (e.g., Wi-Fi, femtocell, or cellular), the induced data stream can be routed through these network backhauls under the control of an SDN controller. Only the receiver can decrypt the data using its private key and then re-organize the data stream coming from multiple network paths, which avoids privacy leakage via compromised APs. Moreover, the proposed scheme is able to realize traffic offloading through the other network paths, which is desirable given the fact that a 5G cellular network will be flooded by a huge volume of mobile traffic [1]. Simply by choosing nearby Wi-Fi or femtocells as different paths for data offloading, the traffic load of a 5G cellular network is relieved through either the unlicensed band of Wi-Fi or reusing the femtocell's band. The proposed SDN-enabled privacy protection mechanism is described in Algorithm 2.

In Algorithm 2, n is the number of network paths that an SDN controller chooses for data transmission, and d_n is the different part of data that will be transmitted in the nth network concurrently. t_r is the data transfer time within the involved networks. T_s is the delay threshold of 5G applications, which means to achieve concurrent privacy protection, this kind of service needs to be finished before T_s to guarantee user experience. For example, email transfer can tolerate long latency, while real-time video and two-way gaming have a very low delay threshold. b_n is the bandwidth allocated by the SDN controller according to the traffic situation of different networks, and V_{sn} is the volume of data that can be transferred in the multiple paths (i.e., offloading networks) within the application delay threshold.

More importantly, the number of paths n here is decided by a trade-off between privacy level, offloading revenue, and system complexity, which is reconfigurable and can easily be set up through an SDN controller application by 5G operators. User privacy protection thus becomes programmable and under the control of SDN, which is especially desirable for future highly diverse communication requirements and application needs.

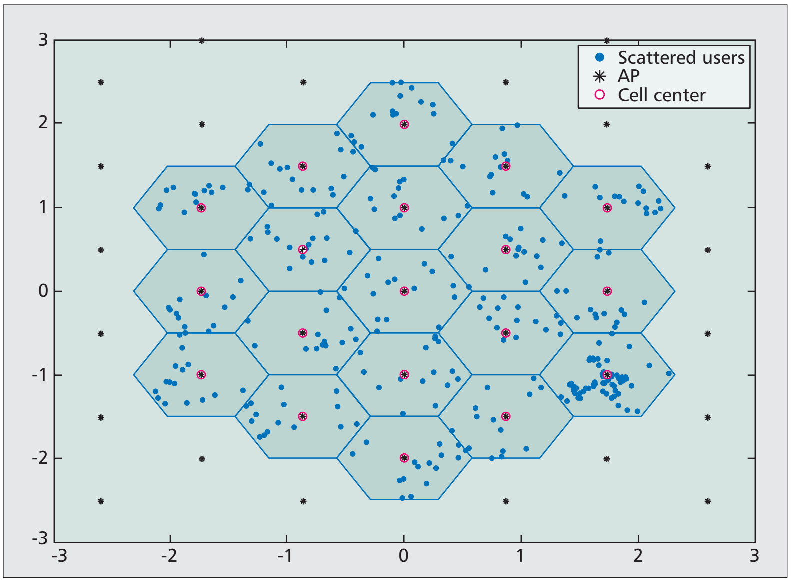


Figure 5. Simulation layout of 5G small cells with proportional axis (1 = 300 m).

Cell layout	Hexagonal grid, 19 cell sites, with wrap-around technique
Cell radius	150m
User mobility speed	3 km/h
User mobility direction	Random
Total number of users	570

Table 1. Simulation parameters of 5G networks.

Performance Analysis

MATLAB simulations of a 5G network with commonly used hexagonal cells are adopted to evaluate the performance of the aforementioned mechanisms in terms of the secure level and latency. A total of 19 small cells in Fig. 5 with an inter-site distance (i.e., distance between two APs) of 300 m is considered in the simulation. Users are randomly distributed around APs, while each UE takes a random walk and changes direction every 5 s. The wrap-around technique (i.e., users moving out of the predefined service area are assumed to enter the area from the other side of the network) is used to avoid boundary effects. The specific simulation parameters are listed in Table 1.

In simulating the proposed SDN-enabled authentication handover, we consider the separation distance between UE and APs, and the moving direction of the UE as the transferred SCI to verify the reliability of the proposed SCI-based authentication handover scheme. From the simulation results, we find that during the monitored user handover process, the probability that any two users have the same distance (with accuracy to the first decimal) to the closest AP is 44 percent. When it comes to the same AP, the probability of two users having the same distance to this AP decreases to 11 percent. Combined with moving direction, signal strength, channel state information, and other user-specific attributes, the probability of UEs with the same SCI could be reduced to virtually 0. Therefore, we believe that the SDN-enabled authentication handover mechanism using SCI transfer is robust to guarantee security with enough SCI attributes. Moreover, it is flexible in setting a security level by different combinations of user-specific attributes.

Authentication handover delays from SDN-enabled handover and the traditional methods are simulated and compared in evaluating the latency performance of the proposed schemes. Without loss of generality, we assume that the data of each user following Poisson arrivals and new users initiate the authentication process when the UE is on the move. In simulating the proposed authentication handover, user-specific SCI is collected and transferred to relevant cells on the projected moving path of the UE under the coordination of the SDN controller. On the other hand, traditional authentication handover protocol requires separate authentication in each network involved in the handover. Here we use two publicly available OpenFlow controllers as representatives to show the performance [14], NOX-MT and Beacon. NOX-MT is a multi-threaded successor of NOX, while Beacon is a Java controller built by David Erickson at Stanford [3].

Figure 6 shows the comparison of authentication delay vs. 5G network utilization rates. Here network utilization is defined as the ratio of total data arrival rate and controller processing rate. Network utilization rate is used as it reflects the different load situations of the network. We can see from Fig. 6 that when the network load is fairly low, authentication delay is not a problem for all different methods. With more arrivals and increased network load, SDN-enabled authentication handover still keeps the latency under 1 ms most of the time, which meets the 5G latency requirement. NOX-MT- and Beacon-enabled solutions perform 30 and 14.29 percent better than traditional handover authentication protocol in latency reduction with the commonly used deployment of an eight-core machine, 2 GHz CPUs, and 32 switches in [14]. It is obvious that the SDN-enabled authentication handover and privacy protection scheme meet the critical latency requirement in 5G, while maintaining the SDN flexibility, programmability, and data offloading capability in further improving the energy efficiency and network management of 5G networks.

Conclusion

With the upcoming multi-tier architecture and small cell deployment, challenges emerge in security provisioning and privacy protection in 5G heterogeneous networks. 5G network security handover needs to be fast, with low complexity due to the reduced cell size and stringent latency constraint. In this article, we review the existing studies and identify current challenges on authentication handover and privacy protection in 5G. In addressing these challenges, we propose SDN-enabled authentication handover and privacy protection through sharing of user-specific security context information among related access points. The proposed SDN-enabled solution not only provides a reconfigurable network management platform, but also simplifies authentication handover in achieving reduced latency. The performance of the proposed schemes have been demonstrated through numerical simulations and examples. We expect that more progress could be made by using emerging SDN-enabled 5G architecture and non-cryptographic techniques to address the 5G challenges of reduced cell size and coexistence of heterogeneous networks. Many interesting related topics, including network complexity, security performance under different attacks, and effective use of security context information, could be explored for SDN-enabled 5G security mechanisms.

References

[1] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018," http://tinyurl.com/b9berc, 2014.

[2] J. Andrews *et al.*, "What Will 5g Be?," *IEEE JSAC*, vol. 32, no. 6, 2014, pp. 1065–82.

[3] B. A. A. Nunes *et al.*, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," *IEEE Commun. Surveys and Tutorials*, vol. 99, Feb. 2014, pp. 1–18.

[4] K.-K. Yap *et al.*, "Blueprint for Introducing Innovation into Wireless Mobile Networks," *Pro. ACM SIGCOMM Wksp.*, 2010, pp. 25–32.

[5] D. He *et al.*, "Secure and Efficient Handover Authentication based on Bilinear Pairing Functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, Jan. 2012, pp. 48–53.

[6] J. Choi and S. Jung. "A Handover Authentication Using Credentials Based on Chameleon Hashing," *IEEE Commun. Letters*, vol. 14, no. 1, 2010, pp. 54–56.

[7] J. Cao *et al.*, "A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks," *Computer Networks*, vol. 56, no. 8, 2012, pp. 2119–31.

[8] L. Cai, S. Machiraju, and H. Chen, "CapAuth: A Capability-Based Handover Scheme," *Proc. INFOCOM*, 2010, pp. 1–5.

[9] L. Chen, J. Ji, and Z. Zhang, *Wireless Security: Models, Threats, and Solutions*, Higher Education Press, 2013.

[10] 3GPP TS 33.401 V11.5.0. 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Rel 11), 2012.

[11] D. He *et al.*, "Security and Efficiency in Roaming Services for Wireless Networks: Challenges, Approaches, and Prospects," *IEEE Commun. Mag.*, vol. 51, no. 2, Feb. 2013, pp. 142–50.

[12] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Commun.*, vol. 17, no. 5, Oct. 2010, pp. 56–62.

[13] 3GPP, Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture, tech. spec. 3G TS 23.203 ver. 9.5.0 (2010-06).

[14] A. Tootoonchian *et al.*, "On Controller Performance in Software-Defined Networks," *Proc. HotICE*, 2012.

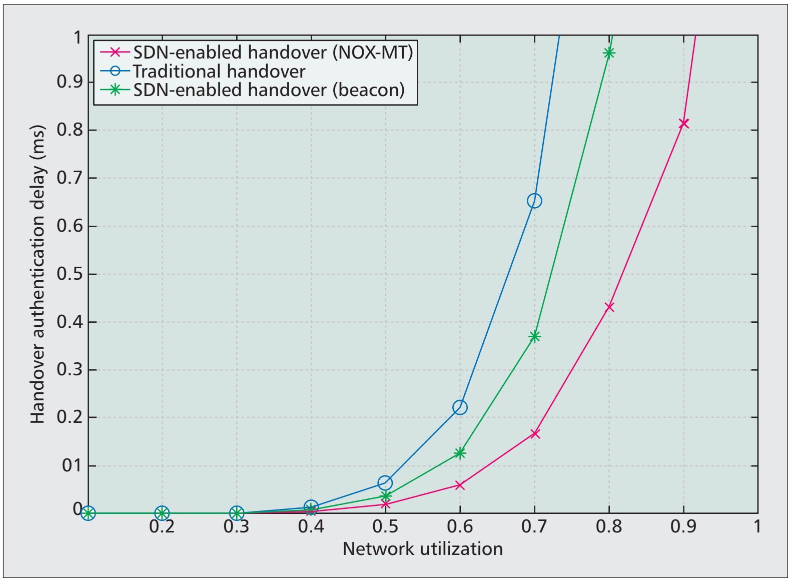


Figure 6. Comparison of authentication delays vs. network utilization rates.

Biographies

Xiaoyu Duan (xduan8@uwo.ca) is a Ph.D. candidate at the Department of Electrical and Computer Engineering, Western University, Canada. She received a B.Sc. in communication engineering from Tianjin University in 2010 and an M.Sc. in signal and information processing from Beijing University of Posts and Telecommunications, China, in 2013. Her research interests include software-defined networking, traffic offloading, self-organizing networks, and communication security in 5G heterogeneous networks.

Xianbin Wang [S'98, M'99, SM'06] (xianbin.wang@uwo.ca) is a professor at Western University and Canada Research Chair in Wireless Communications. He received his Ph.D. degree in electrical and computer engineering from National University of Singapore in 2001. Prior to joining Western, he was with Communications Research Centre Canada as a research scientist/senior research scientist between July 2002 and December 2007. From January 2001 to July 2002, he was a system designer at STMicroelectronics, where he was responsible for system design for DSL and Gigabit Ethernet chipsets. His current research interests include adaptive wireless systems, 5G networks, communications security, and distributed computing systems. He has 200 peer-reviewed journal and conference papers on various communication system design issues, in addition to 24 granted and pending patents and several standard contributions. He is an IEEE Distinguished Lecturer. He has received three IEEE Best Paper Awards. He currently serves as an Associate Editor for *IEEE Wireless Communications Letters*, *IEEE Transactions on Vehicular Technology*, and *IEEE Transactions on Broadcasting*. He was also an Editor for *IEEE Transactions on Wireless Communications* between 2007 and 2011. He has been involved in a number of IEEE conferences including GLOBECOM, ICC, WCNC, VTC, ICME, and CWIT, in different roles such as Symposium Chair, Tutorial Instructor, Track Chair, TPC Chair, and Session Chair.