ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

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

[1]P. Uma, [2]S.Gowtham,[3]P.Sangavi,[4] N.Santhiyabharathi

[1]Assistant Professor, Computer Science and Engineering, Nandha Engineering College, Erode, India.
umamurthi@gmail.com

[2-4]UG Students, Computer Science and Engineering, Nandha Engineering College, Erode, India.

santhiyabharathin@gmail.com

ABSTRACT:

Recently, defined 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 hand - over 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.

Keywords: authentication handover, privacy protection, software defined network.

INTRODUCTION:

Introduce SDN into 5G to enable the proposed authentication handover scheme in coping with the frequent handover authentication in small cells and HetNets. To enable handover between different wireless networks, various authentication servers and protocols are involved due to the closed nature and structure of each network in a HetNet.

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, which is unacceptable for 5G communications. The proposed simplified hand over authentication schemes involves 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. For the same reason, carrying a digital signature is secure but not efficient for dynamic 5G wireless communications. 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, which is unacceptable for 5G communications.

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. We introduce SDN into 5G to enable the proposed authentication handover scheme in coping with the frequent handover authentication in small cells and

HetNets. 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.

We propose an SDN-enabled user-specific secure context information transfer for efficient authentication hand over and privacy protection in 5G to achieve seamless authentication during frequent handovers, while at the same time meeting the privacy and latency requirements effectively. Using a traffic flow template (TFT) filter (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. 1). 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. 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 attacks.

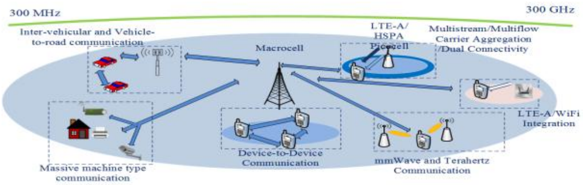
300 MHz
300 GHz
Inter-vehicular and Vehicle-to-road communication
Macrocell
LTE-A/ HSPA Picocell
Multistream/Multiflow Carrier Aggregation /Dual Connectivity
LTE-A/WiFi Integration
Massive machine type communication
Device-to-Device Communication
mmWave and Terahertz Communication

Fig 1: 5G handover

LITERATURESURVEY:

Mobile services based on 4G LTE services are steadily expanding across global markets, providing subscribers with the type of responsive Internet Browsing experience that previously was only possible on wired broadband connections. With more than 200 commercial LTE networks operation in ions are expected to exceed 1.3 billion by the end of 2018. LTE's rapid uptake, based on exponential growth in network data traffic, has opened the industry's eyes to an important reality: the mobile industry must deliver an economically sustainable capacity and performance growth strategy; one that offers increasingly better coverage and a superior user experience at lower cost than existing wireless systems, including LTE. This strategy will be based on a combination of network topology innovations and new terminal capabilities. Simple network economics also require that the industry's strategy enable new services, new applications, and ultimately new opportunities to monetize the user experience, future mobile broadband technologies and standards. (i.e., 5G) the evolutions of the 3GPP's existing LTE standard and IEEE 802.11 standards. 3G/4G network performance is evaluated on "hard" metrics, including peak data rates, coverage, and spectral efficiency.

The 5G Era will see expanded performance metrics centered on the user's quality of experience (QOE), including factors such as ease of connectivity with nearby devices and improved energy efficiency. 5G networks will offer a more user-centric and context-aware experience, delivering personalized content and assistance services. 5G network elements will need to cooperate in new ways to deliver this level of personalization.

DISADVANTAGES:

Existing systems will need to be context-aware, utilizing context information in a real-time manner based on network, devices, applications, existing services, and help provide more user centric and personalized services. For example, networks will need to be more aware of application requirements, QOE metrics, and specific ways to adapt the application flows to meet the QOE needs of the user. There will need to be new interfaces between the application layers and network layers to efficiently adapt both the application source and networking resources to deliver the best QOE for the most users (capacity Application context, such as video, web browsing, gaming, or interactive cloud based applications; QOE metrics; and video specific parameters such as on-demand vs. real-time streaming, bit rate and resolution very low cost throughput .User context, such as user-specific preferences on quality, user activity, user location, and user level of distraction is traffic. Network context, such as congestion/load, air link and backhaul quality, available timely throughputs, and alternative network/ spectrum availability in short time evolution. This ensures that nobody can recover the session key, further enhancing support for non-repudiation. Key update is necessary and benefits users. For example, key update provides an automated method for restricting the amount of data that may be exposed when a session key is compromised.

It should be noted that the session keys used for encryption/decryption have limited lifetimes because the longer a key is used, the greater the chance of a successful attack. The lifetime of a key is determined by many factors including the encryption algorithm used, the degree of confidentiality of the encrypted data, the amount of data encrypted, and the resources of the MN and AP. For example, because WLAN connections can be up for longer periods and have higher transmission rates than vehicular work (VANET) connections, the update of the session encryption key in WLANs needs to be more frequent than in VANETs. Remark: In Hash Hand, a subscriber may cheat the victim by announcing itself as an AP.

To avoid such an impersonation attack, a simple solution is to fix the naming mechanism so that the type of an entity can be inferred by his/her ID information. For example, we can define the first bit of an AP ID to be 0 and the first bit of an MN pseudo-ID to be 1, respectively. Also, as described above, to protect user privacy, MN to constantly change its pseudo-ID in the hand over authentication procedure. Note that the AS does not need to check the reuse of a pseudo-ID. Because the public/private key of each AP is generated with its ID as input, nobody except the AS can modify the ID information and then pass the verification.

Security Analysis and Performance Evaluation of knowing the secrets, SH1 (or) SH1 (IDAP2), no one can generate such a session key. Note that it is computationally infeasible to deduce the master key s from any, sH1)) pair (or any (IDAP2, SH1 (IDAP2)) pair) due to the difficulty of solving the Discrete Logarithm Problem in G. Therefore, even after compromising an arbitrary number of MNs (or APs) and their private keys, the adversary is still unable to calculate the private keys of non-compromised MNs (or non-compromised. Functionality Comparison and Performance fig 2 gives the execution time of the pairing , elliptic curve scalar multiplication (ECSM), hash-to-point, and hash-to-group operations in laptop PCs (with 2 GB RAM) under Ubuntu 11.04 with different computational power. The implementation of all these operations were written in C++ and based on the Multi precision Integer and Rational Arithmetic C/C++ Library (MIRACL). Here Hash Hand Security Analysis Since i = H2 (Mi) · sH1 does not exist in Hash Hand, the design weakness discussed in Appendix B can be avoided.

Here, we analyze the security of Hash Hand to verify whether the requirements mentioned previously are satisfied. The security analysis regarding Requirements can be done. In the following, we focus on key establishment, subscription validation, server authentication and key update of the protocol. Key Establishment As described above, without sharing any secrets, both MN and AP2 can generate their same secret sharing key as follows: MN computes Ki–2 = H2(ê(sH1,H1(IDAP2)))=2(ê(H1, (IDAP2))s) and AP2 computes K2–i = H2(ê(H1, sH1(IDAP2)))= H2(ê(H1,(IDAP2))s). Obviously, without Security and Efficiency Requirements fig 2. Running time of pairing, ECSM, hash-to-point, and hash-to-group operations based on the MIRACL library with pairing.

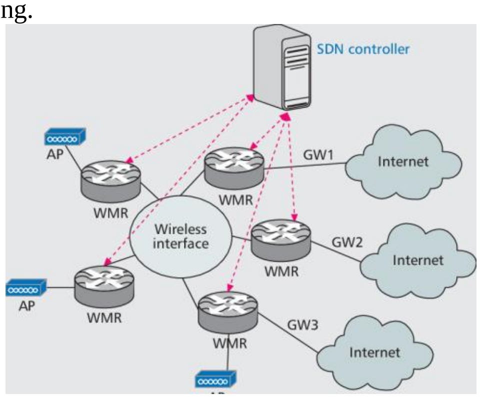

Fig 2: SDN controller

ADVERSARY MODEL:

An adversary can generally launch both outside and inside attacks. In an outside attack, the adversary may eavesdrop, drop, replay, modify transmitted messages, or inject bogus messages to mobile networks. Also, an adversary may launch DOS attacks to exhaust the resources of APs and the AS, and render them less capable of serving legitimate MNs. As an inside attack, the adversary may compromise a number of MNs and APs, and then gain access to their keying materials subject to his/her choice. Handover authentication has been an active field of research, resulting in many interesting protocols. However, as an MN generally has limited power and processing capability, some of the proposed protocols are not suitable for the tight authentication time limit imposed on mobile networks. More-over, some of them do not effectively handle the security and privacy attacks that can easily be launched in the wireless communication environment. A detailed analysis is as follows. To address the above challenges, the efficiency of the three-party approach has been improved by the two-party protocols proposed later in which the need to communicate with AS is completely eliminated. In, Yang et al. present universal authentication protocols to preserve user anonymity against both eavesdroppers and APs. Later, it was demonstrated that the schemes of [6cannot satisfy user intractability, and a novel roaming authentication protocol based on verifier-local revocation group signature technique with backward un link ability was proposed in to remedy this problem. Recently, several lightweight handover authentication schemes have all existing handover authentication protocols can be classified into two categories according to the involvement of the AS. The earlier pro-posed protocols belong to the three-party approach, and involve interactions between the visited AP and the AS, which incur higher authentication delay because at least two additional rounds of communication between the AS and AP are required for the AP to acquire authentication information of an MN from the AS. Moreover, since many APs are served by a single AS, the AS becomes the bottleneck and the single Authentication server been presented through using chameleon hash functions. In these schemes, each AP generates a chameleon hash function on a message from an MN to authenticate the MN. However, there are some security problems with them. For example, the scheme of cannot sup-port user anonymity because an MN sends its own certificate, including its identity, to an AP. In the schemes of, because the effects of a chameleon hash function on the messages from an MN are always identical, anyone can link the messages from an MN. Thus, these two schemes cannot ensure user non intractability.

The Quite recently, proposed a paper handover authentication protocol named Pair Hand shows that it outperforms the above-mentioned protocols on security and efficiency. Pair Hand is very computation and communication-efficient due to two factors. First, it requires only two rounds of communication between an MN and an AP for mutual authentication (i.e., subscription validation and server authentication) and key establishment, while the others require at least three handshakes. Second, it does not require transmission or verification of any certificate as in the traditional public key cryptosystem. In addition, with respect to security functions, compared to the schemes of, Pair Hand relaxes the assumption that the APs are trustworthy and would not disclose users' privacy-related information. The same as Pair Hand, we assume that the lengths of ID_{AP2}, and N are 4, 4, 2, and 4 bytes, respectively. In each experiment, ID_{AP2} and N are randomly picked. It is clear that among all these implementations, all the complex operations based on the MIRA-CL library with eta T pairing are the most efficient. In the following, we just use those operations based on the MIRACL library with T pairing (i.e., Table 1) as an example to illustrate the performance evaluation results. Here we consider the transmission overhead. In Pair Hand (or modified Pair Hand), the lengths of each access request and the response are 105 bytes and 26 bytes, respectively.

However, in Hash Hand, the lengths of each access request {M_i, Aut1} and the response Aut2 are 30 bytes and 20 bytes, respectively. Thus, the transmission delay of Hash Hand is smaller than that of Pair Hand (or modified Pair Hand). With the high transmission rates of wireless networks, the transmission delay of these two protocols can be omitted. For example, today's Wifi devices based on IEEE 802.11a and 802.11g can provide transmission rates up to 54 Mb/s. Additionally, mobile wimax is expected to initially offer up to about 40 Mb/s. Table 4 shows the functionality and performance comparison of Hash Hand and related work. Since the transmission delay is negligible, the authentication latency is defined as the time of cryptography operations. Here we consider that an MN runs on a 1.6 GHz laptop PC while an AP runs on a 2.4 GHz laptop PC based on the execution time.

A handover authentication, a successful handover authentication for Pair hand found to take 19.3733 ms and 10.7694 ms, respectively. Therefore, Hash Hand is efficient when employed on resource-limited devices for mobile net-works. On the other hand, the authentication latency of the modified Pair Hand is due to the pairing operation time on an MN and a visited AP. Using the same MN and AP as above, it has been found that a successful handover authentication for modified Pair Hand takes no less than 818.7ms. Such an authentication process is rather unacceptable in real life applications.

Also, according to the above analysis, compared to Pair Hand, Hash Hand is more efficient in computation and communication overheads of the involved entities. Table 4 also shows the energy consumption at the MN, where it is assumed that an MN runs on a 1.6 GHz processor. It can be calculated as $E_{MN} = T_{MN} \times W$, where E_{MN} is the energy consumption, T_{MN} is the total computation time for handover authentication and W is the CPU maximum power (10.88 W). For communication overhead, we assume that the delivery cost of each authentication message between an MN and an AP is units. All schemes in Table 4 do not involve the AS, and their communication overheads only depend on. Among these schemes, only Pair Hand and Hash Hand require the minimal two handshakes between an MN and an AP. There-fore, they incur the lowest communication overhead. As shown in fig 2, Hash Hand achieves all security requirements and is more efficient than the well-known protocols.

CONCLUSION:

In this paper, we have discussed the security and efficiency requirements of handover authentication protocols. We have reviewed the recent developments of such protocols. Although Pair Hand outperforms all other proposed protocols, it still has some security weaknesses. We have proposed a new secure and efficient handover authentication protocol named Hash-Hand. The security analysis and experimental results have demonstrated that Hash Hand not only eliminates the security vulnerabilities of Pair Hand without sacrificing its merits, but is also more efficient and provides a key update mechanism. Extensive research efforts in the past few years have brought significant advancement in the field of mobile net-working. This results in the emergence of various new mobile networks (e.g., body area sensor networks, BSNs, and vehicle-to-grid networks) that are starting to be deployed in the real world and have great potential to be deployed on a large scale in the near future. Handover authentication modules of these emerging networks have the same or similar requirements.

REFERENCES:

[1]M. Jo et al., "Selfish Attacks and Detection in Cognitive Radio Ad Hoc Networks," IEEE Network, vol. 27, no. 3, May/June, 2013, pp. 46–50.
[2] ETSI, GSM 02.09: Security Aspects, 1993.
[3]3GPP Specification TS 33.102, "3G Security, Security Architecture," Dec. 2002.

[4] C.-C. Chang and H.-C. Tsai, "An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks," IEEE Trans. Wireless Comm., vol. 9, no. 11, Nov. 2010., pp. 3346–53

[5]G. Yang et al., "Universal Authentication Protocols for Anonymous Wire-less Communications," IEEE Trans. Wireless Commun., vol. 9, no. 1, Jan. 2010, pp. 168–74.

[6]D. He et al., "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," IEEE Trans. Wireless Commun., vol. 10, no. 2, Feb. 2011, pp. 431–36.

[7]Q. Han et al., "Efficient and Robust Identity-Based Handoff Authentication in Wireless Networks," Proc. INCoS '12, pp. 222–28.
[8] A. Shen et al., "A lightweight Privacy-Preserving Protocol Using Chameleon Hashing for Secure Vehicular Communications," Proc. IEEE WCNC, 2012, pp. 2543–48.

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

[10] C. Lai et al., "CPAL: A Conditional Privacy-Preserving Authentication with Access Link ability for Roaming Service," IEEE Internet of Things J., vol. 1, no. 1, Feb. 2014, pp. 46–57.

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

[12] M. Avula, S.-G. Lee, and S.-M. Yoo, "Security Framework for Hybrid Wireless Mesh Protocol in Wireless Mesh Networks," KSII Trans. Internet and Info. Sys., vol. 8, no. 1, Jan. 2014, pp. 1982–2004.

[13] D. He et al., "Analysis and Improvement of a Secure and Efficient Hand-over Authentication for Wireless Networks," IEEE Common. Lett., vol. 16, no. 8, Aug. 2012, pp. 1270–73.

[14] S. Yeo et al., "Comments on 'Analysis and Improvement of a Secure and Efficient Handover Authentication Based on Bilinear Pairing