Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks

Jin Cao[a,*], Maode Ma[b], Hui Li[a], Yulong Fu[a], Xuefeng Liu[a]

[a] *State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, China*
[b] *School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore*

ARTICLE INFO

Keywords:
Group-based handover authentication
5G
MMTC
BAN logic
AVISPA and SPAN

ABSTRACT

Future fifth generation (5G) wireless network will be a flexible, open, and highly heterogeneous with densified small cell deployment and overlay coverage. The design of the access authentication for massive machine type communication (mMTC) devices in 5G heterogeneous networks is the challenging issue to achieve 5G applications security due to stringent latency and concurrent access requirements for 5G multi-tier architecture. The current roaming authentication mechanisms between Long Term Evolution-Advanced (LTE-A) network and Wireless Local Area Network (WLAN) proposed by 3GPP incur several protocol attacks with unacceptable delay for real-time mMTC applications. In this paper, we propose secure and efficient group-based handover authentication and re-authentication protocols for mMTC in 5G wireless networks when mMTC devices simultaneously roam into the new networks. Our proposed protocols outperform the standard mechanisms and other related protocols in terms of authentication signaling overhead and bandwidth consumption with robust handover security requirements. The BAN logic and the formal verification tool by using the AVISPA and SPAN show that our proposed protocols are secure against various malicious attacks.

1. Introduction

As the evolutions of the 3GPP's existing Long Term Evolution-Advanced (LTE-A) standard and IEEE 802.11 standards, future fifth generation (5G) mobile network is envisioned to provide more than 10 Gb/s speed, with 1000 times higher wireless area capacity and save up to 90% of energy consumption per service compared with the current 3GPP LTE-A system (Andrews et al., 2014). 5G can also support ultra high definition visual communications, multimedia interactive, mobile industry automation, vehicle connectivity and other applications, and thus achieve a real “Internet of Everything”.

To provide universal high-rate coverage and seamless user experience, 5G wireless network is expected to be a densified heterogeneous network (HetNet) by combining together with LTE-A, WLAN and other radio access technologies to provide a single communication solution. 5G HetNet consists of nodes with different transmission powers and coverage sizes. High power nodes are deployed in large coverage areas including urban, suburban, or rural areas to provide the blanket coverage. Low power nodes (LPNs) are deployed in small coverage areas to enhance the capacity and throughput of HPNs in dense areas with high traffic demands. The tightly coordination between HPNs and LPNs can accomplish the maximum network capacity and coverage benefits of the HetNet deployment. As the most mainstream and most widely used technologies and standards, the interworking between 3GPP LTE-A network as a HPN and WLAN as a LPN can be viewed as most typical 5G HetNet architecture to provide ubiquitous access to user devices. In this paper, we mainly study the efficient interworking between WLAN and LTE-A networks as a 5G enabler.

In the future 5G network, the connection density is going to support at least 1 million connections per squared kilometer and 100 billion

Abbreviation: 5G, fifth generation; 3GPP, 3rd Generation Partnership Project; MTC, Machine Type Communication; mMTC, massive MTC; LTE-A, Long Term Evolution-Advanced; WLAN, Wireless Local Area Network; LPN, Low power node; HPN, High power node; HetNet, heterogeneous network; EAP-AKA, Extensible Authentication Protocol-Authentication and Key Agreement; SN, Serving network; HN, Home network; BS, base station; MD, MTC device; MD_{leader}, MTC group leader; AMAC, Aggregate Message Authentication Code; EPC, Evolved Packet Core; E-UTRAN, Evolved-Universal Terrestrial Radio Access Network; MME, Mobility Management Entity; S-GW, Serving Gateway; PDN-GW, Packet Data Network Gateway; ePDG, Evolved Packet Data Gateway; HAAA, Home Authentication, Authorization and Accounting Server; HSS, Home Subscriber Server; eNB/HeNB, eNodeB/Home eNB; EPS AKA, Evolved Packet System Authentication and Key Agreement; AG, Access Gateway; AAA_{WLAN}, WLAN's Authentication, Authorization and Accounting Server; HIU, Hybrid Interconnection Unit; PLC, Power line communication; AP, Access Point; AVISPA, Automated Validation of Internet Security Protocols and Applications; SPAN, ANimator for AVISPA; HLPSL, High-Level Protocol Specification Language; OFMC, On-the-fly Model-Checker; CL-AtSe, Constraint-Logic-based Attack Searcher; SATMC, SAT-based Model-Checker; TA4SP, Tree Automata based on Automata based on Automatic Approximations for the Analysis of Security Protocol

[*] Corresponding author.
E-mail address: caoj897@gmail.com (J. Cao).

https://doi.org/10.1016/j.jnca.2017.11.009
Received 16 May 2017; Received in revised form 23 September 2017; Accepted 14 November 2017
Available online 16 November 2017

connections in total (IMT, 2015). The support of massive machine type communication (MTC) or IoT devices concurrent connection will be major challenge of the future work for 5G. Wireless World Research Forum (WWRF) has predicted that 7 trillion wireless devices for human and MTCs will be served by wireless communication technologies in 2017 (Nikaein and Krea, 2011). Those massive MTC (mMTC) devices may use heterogeneous radio access systems to communicate, which may result in a lot of interworking problems, such as security mechanisms, seamless handover, and so on. When mMTC devices hand over from 3GPP LTE-A networks to WLAN networks, the handover authentication process is inevitably implemented to ensure the communication security. According to the current 3GPP standard (Generation, 2017), each device needs to execute a full EAP-authentication and key agreement (EAP-AKA) protocol to achieve mutual authentication and key agreement with the network. However, there are two mainly vulnerabilities. One is high intra/inter domain handover authentication and re-authentication delays due to several signaling interactions in the current EAP-AKA mechanisms. It is more serious when mMTC devices roam from LTE-A networks into the coverage of the WLAN networks, which could incur a severe signaling congestion over the network nodes such as eNB, WLAN access point (AP), MME and WLAN server. On the other side, the EAP-AKA protocol can not withstand some protocol attacks including man-in-the-middle attacks (MitM), impersonation attacks, de-synchronization attacks and disclosure of identity information (Cao et al., 2014). Recently, a lot of authentication protocols have been proposed for 3GPP-WLAN interconnection architecture to improve the security of EAP AKA and reduce the re-authentication delays (Shidhani and Leung, 2007; Ntantogian and Xenakis, 2009; ElBouabidi et al., 2012, 2013; El Idrissi et al., 2012; Elbouabidi et al., 2014; Lin et al., 2013; Shen et al., 2014; Kumar and Om, 2015; Wu and Liaw, 2015; Alezabi et al., 2017). By these authentication protocols, there are three participation including UE, serving network (SN) and home network (HN). However, there are a lot of vulnerabilities in these current authentication protocols. First, these three-party protocols require unnecessary multiple rounds of messages exchange between the HSS and UEs, and thus incur a lot of re-authentication delays. Second, these authentication protocols need the HN to be always online and available, which can result in the bottleneck of HN since the SN is far from the HN. In 2014, Elbouabidi et al. (2014) have proposed two re-authentication protocols for secure handover between 3GPP LTE and WLAN networks. By this scheme, the proposed local re-authentication protocol is executed locally in a WLAN network without contacting the authentication server of the HN. However, it still requires several rounds of message exchanges and thus bring a lot of authentication cost. Third, most of the current mechanisms are designed based on improved EAP-AKA protocol, which still inherit its vulnerabilities. Finally, there is no related research work dealing with handover authentication issues for sea of devices in 3GPP LTE-A-WLAN interworking architecture, which still result in high authentication and re-authentication delays and signaling overhead in group communications, since each device must perform a full authentication procedure with the distant authentication server, respectively. Therefore, the design of a secured and fast handover authentication and re-authentication protocol for mMTC in 3GPP LTE-A-WLAN interworking networks is a challenging task.

Until now, there are a lot of research works on the group handover authentication protocols for mass of devices in wireless networks (Fu et al., 2012; Lai et al., 2014; Cao et al., 2015, 2015). Fu et al. (2012) has proposed a group-based handover authentication scheme with privacy protection in the mobile WiMAX network. By this scheme, a group of UEs belonging to the same serving base station (SBS) form a UE group. When the first UE in the UE group visits the target base station (TBS), the TBS can obtain the authentication data for the UE group. Then, the TBS can authenticate other group members directly without contacting the SBS when other group members enter into the TBS. This scheme can largely reduce the communication cost between the SBS and TBS when the rest of group members visits the TBS, since the TBS can obtain all of handover group members' security contexts when the first UE roams to the TBS. However, the scheme in Fu et al. (2012) incurs the authentication traffic between BSs, which is not fit in with the LTE-A-WLAN networks due to the lack of direct interface between the eNBs and the APs. Lai et al. (2014) has proposed a secure and efficient group roaming scheme for MTC between 3GPP and WiMAX networks based on the certificateless aggregate signature technique. By the scheme, the MME/ASN-GW can simultaneously authenticate a group of MTC devices (MDs) in the handover process and obtains an independent session key with each MD. However, the scheme brings a lot of computational costs due to the pairing operations. For inter-E-UTRAN group mobility, Cao et al. have proposed the two group-based handover authentication schemes in Cao et al., (2015a, 2015b), respectively. By the scheme in Cao et al. (2015), when the first MD in the MTC handover group leaves from the current eNB to the target eNB, the current eNB or the current MME transmits all of the handover group members' security contexts to the target eNB or the MME controlling the target eNB. Then, the target eNB can authenticate the rest of the MDs in the MTC handover group locally. This scheme can reduce the signaling cost and the communication cost to the some extent and require only a little computational cost due to the use of symmetric cryptography. By the scheme in Cao et al. (2015b), the target eNB can simultaneously trust the MTC group by checking the multi-signature and AMAC generated by the group leader on behalf of all the group members. This scheme can largely reduce the signaling cost and the communication cost due to the aggregation technique. However, it can bring a lot of computational costs owing to the use of asymmetric cryptography.

To solve the above problems, in this paper, we propose the group-based handover authentication and re-authentication protocols for mMTC between LTE-A networks and WLAN networks, which can be applied to all of application scenarios from LTE-A to WLAN. To avoid the signaling congestion since mMTC devices concurrently request to access to the network, our scheme is inspired by the technique of grouping method and Aggregate MAC (AMAC) to aggregate a lot of handover authentication messages sent from the group of MDs into a single group authentication message and simultaneously authenticate the group of MDs whenever they move into a new network or visited network. At the same time, a distinct session key between each MD and the network is negotiated for the subsequent different communications between the group of MDs and the network. To the best of our knowledge, this is the first group-based handover authentication method in the LTE-A-WLAN heterogeneous networks. Compared with the current standards and other related schemes, our scheme enjoys the following unparalleled features.

1) A large number of handover authentication/re-authentication messages from a group of MDs are aggregated to a single group authentication / re-authentication message. And, the group of MDs can be authenticated by the network at the same time rather than one after the other so that the handover authentication/re-authentication signaling costs and communication costs are largely alleviated, and thus avoid the signaling congestion when a lot of devices simultaneously request to access to a network.
2) A distinct session key can be negotiated by each MD with the network based on different key agreement parameters sent from the group of MDs to guarantee the confidentiality of subsequent data from different MDs.
3) Our scheme is well designed to resist all of the existing attacks including man-in-the-middle attacks (MitM), impersonation attacks, redirection attacks, replay attacks and so on. We have employed the BAN logic to prove the authentication of our proposed protocols and the formal verification tool AVISPA and SPAN to show that our schemes can indeed withstand these