dHSS - Distributed Peer-to-Peer implementation of the LTE HSS based on the Bitcoin/Namecoin architecture

Roger Piqueras Jover *
Bloomberg LP
New York, NY
rpiquerasjov@bloomberg.net

Joshua Lackey
AT&T Security Research Center
New York, NY
joshua.lackey@att.com

***Abstract*—The Home Subscriber Server (HSS) within the packet core of the Long Term Evolution (LTE) is a key node leveraged for essential operations, such as mutual authentication and access control. This centralized node is essential for the overall network operation as it is the cornerstone of the cryptographic functions executed in a mobile network. It stores several parameters for each subscriber, including a copy of the secret key k_i that is securely stored in the Subscriber Identity Module (SIM). The advent of the Internet of Things (IoT) has sparked the concern in the industry on the potential risk of control plane signaling overloads. Due to the traffic characteristics of IoT devices and the potential risk of malfunctioning or compromised devices, there is a potential risk for floods of signaling traffic overwhelming the mobile core network and, in particular, the HSS. Moreover, recent security research has theorized potential attacks against this central core network node that could be launched from a botnet of compromised smartphones. In this paper we theoretically introduce a novel distributed and secure Peer-to-Peer (P2P) implementation of the HSS. Based on the Bitcoin/Namecoin framework, this new architecture drifts away from the symmetric key model of the standard HSS and proposes a robust public key infrastructure. Moreover, it does not rely in central points of failure, it is resilient to signaling overload threats and allows to re-authenticate and re-generate mobile session keys frequently with zero control plane signaling load at the mobile core.**

I. Introduction

Mobile communication networks are rapidly expanding, with connectivity reaching beyond smartphones and tablets. The Internet of Things (IoT) is becoming one of the main evolutionary factors in the mobile ecosystem, with industry forecasts estimating billions of connected devices in just a few years [1]. Novel applications are looming with this pervasive presence of embedded devices providing novel applications, from connected cars [2] to tele-medicine [3].

Both the industry consortiums and standardization communities working in the design of the next generation of mobile networks, 5G, actively embrace the advent of the IoT as both one of the main key drivers and challenges. Mobile networks were designed and optimized to transport human-originated traffic, and hence they are known to suffer from resource utilization inefficiencies when handling M2M communication [4], [5]. It is acknowledged that LTE could be overwhelmed by the surge in both traffic and control plane signaling load [6]–[8]. As a result, one of the main targets for 5G is the ability to provide connectivity for a massive density of connected devices [9].

In terms of potential control plane signaling spikes, the Home Subscriber Server (HSS) is often analyzed as one of the main throttling points [10]. As a matter of fact, there are already efforts in the standardization community proposing mitigations for registration and attachment load spikes at the HSS [11]. Some recent research also investigate similar signaling spikes as a potential security threat [12].

The major efforts in 5G studies focus on a greatly redesigned Radio Access Network (RAN), with enhancements such as millimeter-wave (mmWave) and massive MIMO) [13]. Meanwhile, efforts are also focusing on redesigning the mobile architecture, moving towards a more flat and scalable network operation in terms of control plane signaling traffic. In this context, this paper theoretically introduces a potential new implementation and architecture of the HSS for mobile networks. This fully Distributed HSS (dHSS) is implemented as a Peer to Peer (P2P) distributed ledger, resulting in a non centralized packet core node. This removes the potential centralized point of failure of the HSS in a traditional architecture, which is known to be a great challenge for the expected massive distribution of the IoT [8].

The dHSS leverages the architecture of the blockchain in Bitcoin [14] enhanced with the database-like properties of Namecoin [15]. The dHSS provides the same functionality expected from the HSS in a fully distributed way, which allows to locally authenticate mobile devices, with zero control plane traffic at the packet core, in the scenario of all the eNodeBs belonging to the dHSS P2P network. Nevertheless, the dHSS implementation is challenging due to the fact that it changes the key distribution paradigm in mobile networks, moving from a symmetric key scenario to a public key architecture.

The remainder of this paper introduces the concept of the dHSS in the context of the mobile packet core. Section II presents some background regarding the operation of LTE mobile networks, and Section III presents the motivation for the dHSS in terms of mobile network security. Finally, Section IV overviews the implementation and characteristics of the dHSS and Section V concludes the paper.

II. LTE mobile network operation

Release 8 of the 3GPP (3rd Generation Partnership Project) standards resulted in the inception of LTE mobile networks,

*R. Piqueras Jover was a member of the AT&T Security Research Center when this work was done.

aimed to provide IP connectivity between mobile devices and the Internet based on the architecture shown in Figure 1. The proposed network architecture is split into two separate sections: the Radio Access Network (RAN) and the core network, referred to as the Evolved Packet Core (EPC).

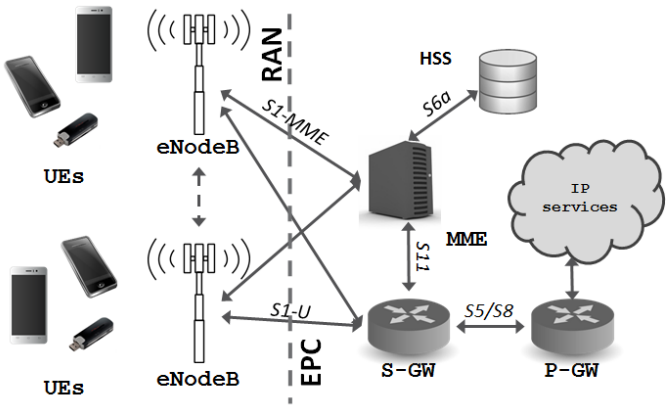

Fig. 1. LTE network architecture

The RAN is composed by the mobile terminals (known as User Equipment - UE) and the eNodeBs, or LTE base stations. The access segment of an LTE mobile network assigns and manages radio resources for the UEs, and is also in charge of access control and handoffs between adjacent eNodeBs. The EPC, in turn, establishes and manages the point-to-point IP connectivity between UEs and the Internet through a tunnel or bearer through the mobile core. Within the EPC one finds the following nodes: the Serving Gateway (SGW) and the PDN Gateway (PGW), which anchor the point-to-point bearer and route data traffic between a UE and the Internet. The Mobility Management Entity (MME) is in charge of the control plane, managing bearer dynamics, as well as other network functions. Finally, in order to authenticate the UEs and perform essential cryptographic operations, the MME leverages subscriber records stored in the HSS.

In order to provide connectivity to mobile devices and manage the network resources, LTE systems execute certain signaling processes, known as Non Access Stratum (NAS) functions [16]. The execution of NAS operations is initiated and coordinated by means of *control plane signaling* messages among multiple network nodes.

Whenever a mobile device needs to attach and authenticate with the mobile network, a series of steps are executed. The same steps are required whenever the communication session key needs to be refreshed. Assuming that the UE has acquired both time and frequency synchronization, a Random Access procedure is executed so radio resources can be assigned to the UE, which is by default on an *idle* mode. Then, the Radio Resource Control (RRC) connection is established with the eNodeB [17]. At this point, the NAS identity and authentication procedures are executed between the UE and the MME, which in turn communicates with the HSS. This final step requires a large number of control plane signaling messages being exchanged among various EPC nodes, which result in a data traffic bearer being established and the device transitioning to a *connected* state.

III. Mobile network security

Security research throughout industry and academia has intensified over the last few years. The widespread availability of low-cost, open-source platforms has resulted in the successful identification of potential threats to legacy mobile networks. The majority of security research has mainly focused on Second and Third Generation mobile networks (2G and 3G). Some of these potential threats are also being investigated in the context of next-generation LTE mobility networks.

Security researchers and the standardization community have identified over the last few years a series of potential overloading threats against the control plane that could theoretically overload the EPC and impact the Quality of Service (QoS) of mobile phone customers. The authors of [18] introduced the first theoretical control plane signaling overload threat against cellular networks. The results indicated that a low-volume traffic wave, consisting of small data packets addressed to a large number of mobile devices, could theoretically be leveraged to force a large number of RRC state transitions idle-connected-idle. This would result in a spike of signaling load at the EPC. This could potentially overload the packet core of a mobile network.

Similarly, the authors of [12] discussed theoretical attacks that would target the Home Location Register (HLR), with similar functionality to the HSS but in the context of 3G networks. The goal of this threat is to overload the HSS with control plane signaling requests to impact, slow down and potentially block its operation. Further signaling-based attacks against 3G networks were introduced in [19]. Such threats could potentially be triggered from within the mobile network by means of a botnet of compromised smartphones. The authors of [20] discussed feasible techniques and platforms to build and operate such a botnet, including potential command and control channels.

Recent research work has explored these potential attacks in the context of LTE. A simulation study of a potential attack launched by a botnet of mobile devices is presented in [21]. The paper discusses the potential overloading of the LTE RAN resources that a botnet could generate. Other LTE security research works have recently investigated ways to optimize the control plane to mitigate overloading attacks [22].

Although there are no recorded instances of control plane signaling attacks in major cellular networks, similar signaling overload effects have been observed over the last few years [23]–[27]. These were triggered by non-malicious applications or devices with a suboptimal wireless resource utilization.

Control plane signaling overloads at the HSS are one of the main security use cases under analysis in the standardization community [11]. Beyond botnets of compromised smartphones, further scenarios that could lead to such an threat are being analyzed. The advent of the Internet of Things (IoT), with forecasts of billions of embedded devices joining mobile cellular networks, increases the concern of large botnets of compromised or misbehaving Machine to Machine (M2M) connected appliances. 3GPP also considers other potential triggers for an HSS saturation, such as a node failure [11]. In the event of a node failure, a large number of UEs would be disconnected from the network and potentially generate a

surge of signaling messages upon re-attaching and attempting to authenticate with the HSS.

A. Cellular traffic encryption challenges

Security researchers demonstrated recently the weaknesses of the encryption scheme in legacy GSM (Global System for Mobile Communications) [28]. The outdated encryption algorithms leveraged in 2G wireless links are vulnerable to brute force attacks, allowing a skilled attacker with the right tools to extract the session key within minutes. As a result, over the air traffic can be decrypted and the SIM can be cloned for as long as the session key does not change. Cellular encryption is also vulnerable due to the fact that they are based on a symmetric key model. Note, though, that the majority of IP-based services provide extra encryption at the application layer.

Although both 3G and LTE networks implement a much more resilient encryption scheme, session key regeneration is a necessary measure to guarantee the security and privacy wireless cellular traffic [29]. This session key is derived from the secret key k_i stored within the SIM and the HSS and obtained through a series of cryptographic operations inherent to the mobile authentication NAS procedure. Therefore, expensive control plane operations have to be executed in the EPC, with a large number of signaling messages. As a result, in order to minimize the threat of a signaling traffic storm, it is not possible to re-authenticate UEs and refresh their session key as often as it would be ideal.

In most cellular networks, rekeying does not occur until the mobile device is disconnected from the network and, in some events, when the phone moves to a new geographical area under a different MME in the case of LTE. The current trend of smart phone users of never shutting the phone off exacerbates the problem further, resulting in the session key being refreshed very rarely.

IV. Distributed HSS architecture and operation

In this document, a novel alternative implementation of the LTE HSS is proposed. This HSS architecture is fully distributed, preventing the challenge of a centralized EPC node, which could potentially be a single point of failure overloaded by a malicious attack or a control plane signaling traffic anomaly. The proposed system is implemented as a P2P distributed database (DDB), leveraging the architecture of the blockchain in Bitcoin [14] and the database properties of Namecoin [15].

The distributed HSS (dHSS) is designed to provide the same functionality of the LTE HSS, with no loss in security and with enhanced resilience against control plane signaling spikes and mobile botnet threats. Moreover, the dHSS is scalable and, thus, suitable for the spreading of the IoT, as this architecture performs the attach and authentication operations with zero signaling load at the EPC. Note that, given this lack of signaling at the packet core for the authentication operation, the dHSS allows to refresh the session key as often as desired, for example each time a UE transitions from *idle* to *connected* RRC state.

Moreover, the dHSS drifts away from the symmetric key architecture of the HLR and HSS, vulnerable to key leaks, and implements a public-private key infrastructure. Therefore, only one of the two main keys needs to be protected.

Although the dHSS is envisioned in the context of LTE mobile networks, it could trivially be implemented as an alternative method for the 2G/3G Home Location Register (HLR).

A. Bitcoin and Namecoin

Bitcoin is a decentralized digital currency and payment method introduced in 2008 by an unknown author under a pseudonym [14] and released in software in 2009. This peer-to-peer payment system does not rely on trusted third parties as users, the network nodes, can verify transactions, which are stored in a public ledger: the block chain.

The block chain is a distributed data base of transactions, with each member of the P2P network storing locally a copy. Transactions, as defined in the Bitcoin documentation, is comprised of a series and fields, an input script and an output script [30]. Transactions on this distributed data base are validated and recorded by means of computer power offered by the mining network nodes. In average, every few minutes a new set of verified transactions, known as a block, is assembled, appended to the block chain and published to the rest of the network, providing the means to avoid double spending.

Namecoin is a fork of Bitcoin and is based on the same proof-of-work architecture. By means of adding extra input and output scripts to the transactions, the block chain of Namecoin inserting data into the transactions. Specifically, it allows storing id-value pairs. Among other uses cases, Namecoin is widely used in the censorship evading top level domain .bit [15].

B. dHSS architecture

The dHSS leverages the Bitcoin blockchain, the distributed database in the bitcoin infrastructure. Alternatively, the P2P network of nodes involved in the dHSS operation could run their own internal distributed blockchain. In the case of utilizing the existing blockchain, the system would take advantage of the millions of nodes already contributing and monitoring the security of its transactions.

In the dHSS architecture, the eNodeBs of the cellular operator A form the - public or internal - Bitcoin P2P network. Within the network, they all share a DDB of transactions, the blockchain. As with the Bitcoin operation, although a compromised network node could attempt to corrupt the DDB, this would not be possible unless the majority of nodes were compromised [14]. Moreover, in the event of a node (i.e. an eNodeB) being down or overwhelmed by an overloading attack, the dHSS operation would be unaltered and only UEs under the coverage of the victim eNodeB would be affected.

In order to enhance the resiliency and processing speed of an internal dHSS blockchain, other network nodes could be added to the P2P network, though they would not execut the dHSS functionality.

The dHSS architecture herein defined assumes a strong public-secret key encryption scheme with strong keys (i.e.

2048 bits). The DDB - the blockchain - contains transactions, as defined in the Namecoin framework, used to register $\{value, key\}$ pairs and optional extra flags. For example, a given transactions in the dHSS DDB registers id of node j and its corresponding public key k_j^p as the pair $\{j, k_j^p\}$. These transactions must be originated by the cellular operator A, which signs them with its secret key k_A^s. In turn, the public key of the network operator k_A^p is utilized to verify transactions and validate that they were created and inserted into the DDB by the network operator. How to protect the secret key k_A^s is outside of the scope of this paper. The network operator could store it in the same secure systems where sensitive customer records and information are stored. Standard cryptographic methods with multiple keys instead of one could be leveraged as well, such that several keys should be stolen before the overall k_A^s is compromised.

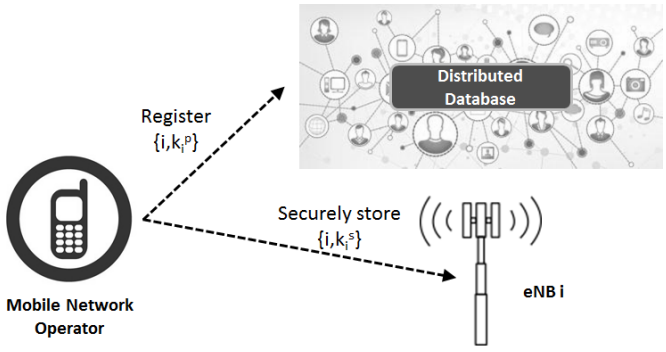

Fig. 2. eNodeB registration

A dHSS considers two types of transactions in the blockchain: registration of an eNodeB and registration of a SIM.

*1) **eNodeB registration**:* Although legacy cellular networks are vulnerable to Man in the Middle (MitM) attacks [31], 3G and LTE networks implement mutual authentication. On top of authenticating the mobile subscriber, the eNodeB must authenticate itself to the UE as well. To fulfill this requirement, the network operator registers each eNodeB on its DDB, as depicted in Figure 2. In the process of registering eNodeB i, the transaction for the pair $\{eNB_i, K_i^p\}$ is signed with K_A^s and stored in the blockchain, where K_i^p is the public key of eNodeB i. In parallel, the corresponding secret key K_i^s is securely stored within eNodeB i, for example inside a hardware secure compartment or Trusted Platform Module (TPM) [32]. For notation clarity, keys for eNodeBs are defined with an upper case 'K' as opposed to a lower case 'k' for the SIM keys.

*2) **SIM registration**:* The process of registering a SIM on the dHSS is identical to the eNodeB registration, as observed in Figure 3. The network operator signs and stores the transaction $\{IMSI_j, k_j^p\}$ in the DDB. In this case, the identifier of user j can be mapped to the International Mobile Subscriber Identifier (IMSI) and k_j^p is the public key of user j. Similarly, the operator would securely store $IMSI_j$ and the corresponding secret key k_j^s in the SIM. This is a common operation in standard cellular networks. In order to allow a mobile terminal to independently verify transactions, the mobile operator also burns its public key k_A^p on the SIM, as it will be detailed in Section IV-C.

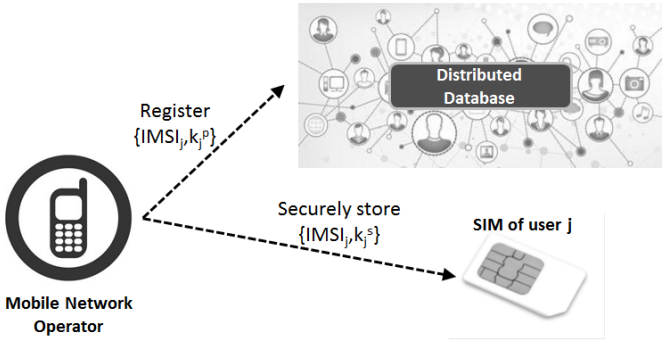

Fig. 3. SIM registration

Note that, in the context of the dHSS operation, the IMSI is stored and always transmitted in the clear. This could potentially be exploited to force location privacy leaks [28]. In order to prevent such threat, a new SIM identifier $IMSI_j(t)$ could be generated each time t a new session key is derived. As a result, an attacker would have to constantly monitor the traffic of a given user in order to be able to know its IMSI at all time and, thus, determine its location.

In the event of a secret key being leaked or potentially brute-forced, a new public-secret key pair would be registered on the DDB, discarding the compromised key. Therefore, the dHSS system can restore from an eventual yet highly unlikely SIM secret key brute force atttack.

C. Functionality of the dHSS

The dHSS is designed to implement the same functions of a regular HSS in a distributed way with zero control plane signaling at the EPC. These functionality must be achieved while maintaining the security and integrity of the system. The main functions implemented by the LTE HSS, as defined in [33], are mutual authentication, access control, session key maintenance and assisting with roaming users.

*1) **Mutual authentication**:* The dHSS architecture detailed in Section IV-B provides the means to execute mutual authentication through a simple cryptographic handshake. Figure 4 depicts a sample handshake for mutual authentication and session key generation. In this case, the UE j sends $IMSI_j$ to eNodeB i. Given this $IMSI_j$, eNodeB i queries the DDB for a verifiable transaction from the MNO (i.e. a transaction signed with k_A^s) that contains $IMSI_j$. From that transaction, the eNB extracts the public key k_j^p of the user's SIM, linked to its identity $IMSI_j$.

At this point, the eNodeB i generates a random nonce N, encrypts it with the SIM's public key k_j^p and sends it to the UE. In parallel, eNodeB i forwards the verifiable transaction $\{i, K_i^p\}$ to the UE. Note that, at this connection stage, the mobile device does not have a connection to the network yet, so it cannot query for the eNodeB identifier i on its own. Although the eNodeB provides the UE with its own identifying transaction, there is no threat with potential rogue base stations. Given that the SIM is pre-provisioned with the operator's public key k_A^p, as described in Section IV-B, only verifiable transactions will be considered. These are the transactions that were signed with the operator's secret key k_A^s. At most, a rogue

base station could forward a verifiable transaction identifying a legitimate eNodeB. However, the attacker would not be able to decrypt the subsequent traffic encrypted with the key K_i^p that the mobile device would extract from the transaction.

In the next step, the mobile device decrypts the nonce N with its secret key k_j^s, verifies the transaction identifying eNodeB i and generates a random nonce M. Both nonces are then encrypted with the public key of eNodeB i and transmitted back. At the final stage, eNodeb i decrypts the message, authenticates SIM i by checking the first nonce N and identifies itself by transmitting back, encrypted, nonce M.

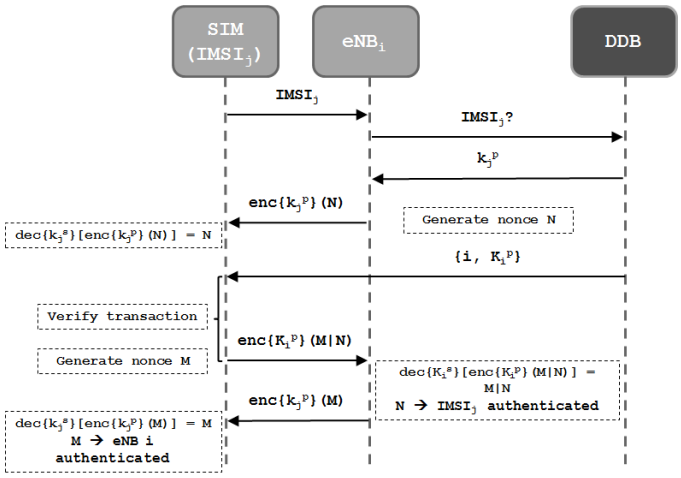

Fig. 4. Mutual authentication process with dHSS

*2) **Session key generation**:* The mutual authentication execution with the dHSS results in two random nonces securely shared among UE j and eNodeB i, such that a session key can be derived from them by means of a standard cryptographic primitive. Once the algorithm is run in the initial attach, the subsequent session key derivations do not require the eNodeB to query in the DDB for $IMSI_j$ and to forward to the UE its identifying blockchain transaction, under the assumption that there has not been a handover to a new cell. This process does not result in any control plane signaling at the EPC, as no further queries to the DDB would be required. Therefore, the mobile network could execute mutual authentication and session key regeneration frequently without a spike in signaling load. The algorithm would, by definition, run each time UE j camped on a new cell as it moves. Also, a new session key could be derived each time UE j transitions from idle to connected *RRC* state. Therefore, a new session key ks would be generated very frequently, satisfying the motivation of the need for frequent rekeying in mobile networks.

*3) **Network access control**:* The Namecoin architecture provides the means to register a series of flags or extra fields along with a {key,identifier} pair. These flags can be leveraged in the access control functionality of the dHSS. For example, mobile network operators block or throttle data traffic speeds for customers who have filed their monthly data cap. Similarly, all communications of a given SIM card are fully blocked (i.e. the account is blocked) in situations of mobile fraud, such as SMS spam [34]. In turn, certain IoT applications base their communications mostly, or exclusively, on SMSs (Short Message Service). All these particular access characteristics (blocked, throttled or only access to a subset of traffic channels) are implemented on the dHSS by means of the flags in Namecoin transactions.

*4) **Roaming and standard HSS operation**:* Unless the dHSS architecture became standardized and part of the global mobile connectivity and routing, implementing a dHSS-based mobile architecture would not be compatible with current smart-phones and SIM cards. For example, a foreign user roaming into the network of cellular operator A would not be able to attach and connect a mobile device. In order to guarantee backwards compatibility with standard LTE deployments and roaming devices, the eNodeB routes the HSS functionality according to the type of device and SIM card. In parallel, either a range of IMSIs could be allocated for dHSS-compatible SIMs or a bit within the 15 digit IMSI could indicate the nature of the SIM. Based on this flag, the eNodeB would perform the mutual authentication by means of the DDB or through the EPC, as described in Figure 5. In the case of a roaming user, the EPC would interface with the home provider of the user via the SS7 network [35].

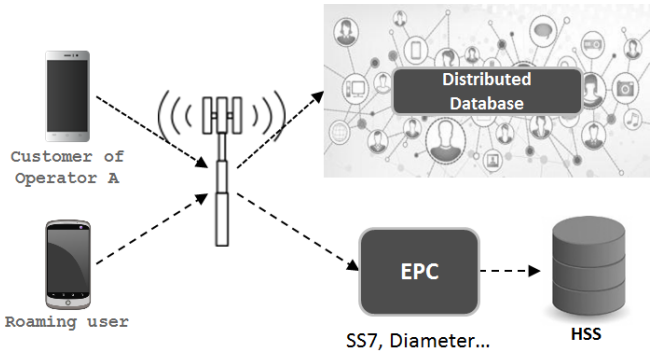

Fig. 5. Roaming and compatibility with standard HSS

D. Latency and scalability of the dHSS

It is important to note a few details regarding the scalability and latency of the dHSS implementation. A new transaction on the DDB would only occur each time a new SIM or eNodeB is registered or when the registration of an existing one is modified. Therefore, the number of transactions per unit of time would be drastically smaller than in, for example, the Bitcoin ledger. Consequently, the network load would be much lower than in fully functional blockhain applications.

The dHSS is highly scalable as, an increase in the number of mobile devices does not generate an increase in control plane load. Essentially, adding N SIMs to the network would require initially to register N new transactions to the DDB. However, from this point on, the operation of the network will be local at each eNodeB and limited to queries to the local copy of the DDB.

In terms of latency, as any other blockchain-based ledger, there is a substantial delay until a transaction is accepted by the network. As a result, once a user got a new SIM card in the store, it would take a few minutes until the device was operational. Likewise, a new eNodeB added to the DDB would not be operational for a few minutes. However, the authentication and key derivation functions do not require

any transactions to be added to the network. In order to authenticate a user, simple query functions are executed on the DDB, resulting in no latency. As a matter of fact, given that each eNodeB has a local copy of the ledger, the latency to authenticate a user is close to zero and much smaller than the latency in a standard EPC implementation.

V. Conclusions

As industry consortium and standards bodies actively work on designing the fundamentals of the next generation 5G mobile networks, control plane signaling scalability is still one of the main challenges in mobile networks. Despite the tremendous capacity gains achieved with mmWave and massive MIMO, the current bearer-based architecture is still a challenges for the goal of deploying billions of IoT connected devices over 5G networks.

In this paper we introduced a new potential architecture to provide the HSS functionality in a mobile core network in a fully distributed way, based on the blockchain of cryptocurrencies enhanced with the properties of Namecoin. This implementation removes the central point of failure that the HSS becomes under high control plane load situations. Moreover, the P2P implementation of the dHSS potentially provides the means for local mobile device authentication without requiring costly signaling message exchanges at the packet core. As a result, this new architecture could be beneficial within the overall framework of the redesigned 5G packet core architecture.

References

[1] "More than 50 billion connected devices," Ericsson, Ericsson White Paper, February 2011, http://goo.gl/Xi7dE1.

[2] "The Connected Car: Making Cars Smarter and Safer," AT&T, 2014, http://goo.gl/PJYp3g.

[3] A. Jara, M. Zamora, and A. Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments," in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*, jan. 2010, pp. 1 –5.

[4] T. Petsch, S. Khan Marwat, Y. Zakit, and C. Gorg, "Influence of Future M2M Communication on the LTE system," in *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*. IEEE, 2013, pp. 1–4.

[5] R. Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, Atlantic City, NJ, June 2013, pp. 1–9.

[6] A. Prasad, "3GPP SAE-LTE Security," in *NIKSUN WWSMC*, July 2011.

[7] M. Jaber, N. Kouzayha, Z. Dawy, and A. Kayssi, "On cellular network planning and operation with m2m signalling and security considerations," in *Communications Workshops (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 429–434.

[8] J. Jermyn, R. P. Jover, I. Murynets, M. Istomin, and S. Stolfo, "Scalability of machine to machine systems and the internet of things on lte mobile networks," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*. IEEE, 2015, pp. 1–9.

[9] "5G Radio Access: Requirements, Concept and Technologies," NTT Docomo, 2014, http://goo.gl/L72689.

[10] C.-K. Han, H.-K. Choi, J. Woo zBaek, and H. W. Lee, "Evaluation of authentication signaling loads in 3GPP LTE/SAE networks," in *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on*. IEEE, 2009, pp. 37–44.

[11] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects, "Study on Core Network Overload and Solutions. 3GPP TR 23.843," vol. v0.7.0, 2012.

[12] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core," in *Proceedings of the 16th ACM conference on Computer and communications security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 223–234.

[13] J. Thompson, X. Ge, H.-C. Wu, R. Irmer, H. Jiang, G. Fettweis, and S. Alamouti, "Guest Editorial on 5G Wireless Communication Systems: Prospects and Challenges," in *IEEE Communications Magazine*, vol. 52, February 2014, pp. 62–64.

[14] "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008, http://goo.gl/X1EivQ.

[15] "Namecoin - A decentralized open source information registration and transfer system based on the Bitcoin cryptocurrency," Tech. Rep., http://namecoin.info/.

[16] S. Sesia, M. Baker, and I. Toufik, *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Wiley, 2009.

[17] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, "Evolved Universal Terrestrial Radio Access (E-UTRA) - Radio Resource Control (RRC) - Protocol Specification. 3GPP TS 36.331," vol. v8.20.0, 2012.

[18] P. Lee, T. Bu, and T. Woo, "On the Detection of Signaling DoS Attacks on 3G Wireless Networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, May 2007.

[19] G. Kambourakis, C. Kolias, S. Gritzalis, and J. Park, "DoS attacks exploiting signaling in UMTS and IMS," *Computer Communications*, vol. 34, no. 3, pp. 226–235, 2011.

[20] C. Mulliner and J.-P. Seifert, "Rise of the iBots: 0wning a telco network," in *Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware)*, 2010.

[21] M. Khosroshahy, D. Qiu, M. Ali, and K. Mustafa, "Botnets in 4g cellular networks: Platforms to launch ddos attacks against the air interface," in *Mobile and Wireless Networking (MoWNeT), 2013 International Conference on Selected Topics in*. IEEE, 2013, pp. 30–35.

[22] J. Cao, M. Ma, H. Li, and Y. Zhang, "A survey on security aspects for lte and lte-a networks," *IEEE Communications Surveys and Tutorials*.

[23] M. Dano, "The Android IM app that brought T-Mobile's network to its knees," Fierce Wireless, October 2010, http://goo.gl/O3qsG.

[24] "Signal storm caused Telenor outages," Norway News in English, June 2011, http://goo.gl/pQup8e.

[25] C. Gabriel, "DoCoMo demands Google's help with signalling storm," Rethink Wireless, January 2012, http://goo.gl/dpLwyW.

[26] E. Savitz, "How The New iPad Creates 'Signaling Storm' For Carriers," Forbes, March 2012, http://goo.gl/TzsNmc.

[27] A. Gulati, "A signaling storm is gathering Is your packet core ready?" Nokia, December 2012, https://goo.gl/6H5lJm.

[28] K. Nohl and S. Munaut, "Wideband GSM sniffing," in *In 27th Chaos Communication Congress*, 2010, http://goo.gl/wT5tz.

[29] K. Nohl, "Attacking phone privacy," *Black Hat USA*, 2010.

[30] "Bitcoin Wiki: Protocol documentation," Tech. Rep., https://goo.gl/WxAKt8.

[31] U. Meyer and S. Wetzel, "On the impact of gsm encryption and man-in-the-middle attacks on the security of interoperating gsm/umts networks," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, vol. 4. IEEE, 2004, pp. 2876–2883.

[32] T. Morris, "Trusted platform module," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 1332–1335.

[33] Universal Mobile Telecommunications System (UMTS) - LTE, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) - Stage 3. 3GPP TS 24.301," vol. v9.11.0, 2013.

[34] I. Murynets and R. Piqueras Jover, "Crime scene investigation: Sms spam data analysis," in *Proceedings of the 2012 ACM conference on Internet measurement conference*. ACM, 2012, pp. 441–452.

[35] L. Dryburgh and J. Hewett, *Signaling system No. 7 (SS7/C7): protocol, architecture, and applications*. Cisco press, 2003.