Journal of Theoretical and Applied Information Technology
15th July 2017. Vol.95. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUTHENTICATION GROUPS WITH PRIVACY-PROTECTION OF MACHINE-TO- MACHINE IN LTE/LTE-A NETWORKS

[1]HAQI KHALID, [2]KWEH YEAH LUN, [3]MOHAMED OTHMAN, [4]IDAWATY AHMAD

[1]University Putra Malaysia (UPM), Department of Computer Science

[2]University Putra Malaysia (UPM), Department of Computer Science

[3]University Putra Malaysia (UPM), Department of Computer Science

[4]University Putra Malaysia (UPM), Department of Computer Science

E-mail: [1]haqikhalid@gmail.com, [2]yeah_lun@upm.edu.my, [3]mothman@fsktm.upm.edu.my, [4]idawaty@upm.edu.my.

ABSTRACT

Machine-type Communication (MTC) is a form of data communication which involves one or more entities that do not necessarily need human interaction, which has become the hotspot in industry area. Furthermore, Machine-Type Communication (MTC) has shown the advantages, including better coverage and lower network deployment cost, which makes it become the hotspot in industry area. However, the current cellular network is designed for human-to-human communication (H2H), and less optimal for machine-to-machine, machine-to- human or human-to-machine applications. In addition, current cellular network is less optimal for MTC applications, and now facing some urgent issues, e.g. congestion and overload caused by the access of masses of MTC devices. This paper shows the techniques that used in MTC for LTE/LTE-A networks to enhance the authentication protocols with reduce signaling overhead and computational cost. Furthermore, this work discussed the problems that causing signaling overload in the core network especially, when a group of MTCD try to get authenticate to the system at the same time.

Keywords: *Machine-Type-Communication, Authentication Groups, Privacy-Preserving, Signaling Congestion, LTE/LTE-Advanced Networks.*

1. INTRODUCTION

Machine type communication (MTC), also known as Machine-to-Machine (M2M), can realize intelligent and interactive seamless connection among people, machine and system via wireless communication technologies [1]. Recent years have witnessed a tremendous growth of mobile user population and multimedia service, which are causing a severe traffic overload problem in the traditional cellular network. Device-to-device (D2D) communication has been proposed to be a promising data offloading solution and spectrum efficiency enhancement methods due to its inherent characteristics, e.g. improve resource utilization, enhancing user's throughput, extending battery lifetime, etc. [2]. The purpose of the MTC technology is to enable all of machineries and equipment networking and communication ability, which is a main way of the Internet of Things (IoT) applications [1]. Concerning wireless network security, authentication is one of first measure that must be taken to validate users or the system. Due to its characteristics of low power, low cost, and no human intervention, the development of MTC has quickly become the driving force of the market for a mass of real-time network applications, such as public safety, environmental monitoring, and so on [15]. Different from the common user equipment's (UEs), MTC devices (MTCDs) bring some new requirements including lower power consumption and mass devices transmission, and the number of MTCDs may increase quickly [15]. In addition, when a group of n MTC devices authenticate themselves to a core network simultaneous authentication of individual MTC devices can burden signaling on the network. Its efficiency drops significantly because of repetitive invocation of costly authentication signaling [27]. Meanwhile, cyber security is of paramount importance in MTC; if MTC devices cannot securely access the networks through efficient authentication, all applications involving MTC cannot be widely accepted. A large number of MTC devices

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

accessing the network simultaneously will cause a severe authentication signaling congestion [19]. With a widely range of potential applications, many standards forums and organizations have developed and enhanced the current technologies in order to enables the MTC applications. In particular, the third Generation Partnership Project (3GPP) is becoming increasingly active in this area with several work items defined on MTC, especially for Long Term Evolution (LTE/LTE-A) networks [26]. The difficulties in this platform is belong to the requests of the large number of MTC devices because each MTCDs needs an independent complete access authentication process with core network, which may cause serious signaling congestion in the core network [34]. In particular, avoiding denial of service attack by filtering some illegal devices in the first four procedure of the mutual authentication is one of the solution that could provide robust privacy-preserving for each MTCD (including anonymity, unlinkability, and traceability) [34].

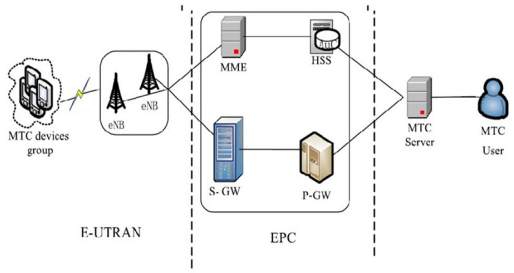

Figure1. Machine-Type Communication (MTC) Model In The Long-Term Evolution (LTE)/LTE Advanced Networks.

Table 1: Components of Machine type communication in LTE/LTE-A networks.

Entity	Abbreviation
Machine-Type Communication Devices	MTC Devices
Evolved Node B	eNB
Mobility Management Entity	MME
Serving Gateway	S-GW
Home Subscriber Server	HSS
Packet Data network Gateway	P-GW
Evolved Packet Core	EPC

Compared with other wireless networks, the long-term evolution/long-term evolution advanced (LTE/LTE-A) network can provide higher data rates, lower access latency, and more flexible bandwidth, so it can served as an ideal platform for MTC technology to provide strong support for the development of MTC [34]. In this paper, we discussed the problems that may happen to the authentication process for MTC in LTE/LTE-A Networks. Likewise, we summarized the previous solutions for MTC in LTE/LTE-A networks in group authentication protocols and the signaling congestion that the core network face while a large number of MTC devices need to authenticate to the system

2. AUTHENTICATION AND KEY AGREEMENT

In 2000, Ateniese et al. studied the problem of the authenticated key agreement in dynamic peer groups with the emphasis on efficient and provably secure key authentication, key confirmation, and integrity. It begins by considering two-party authenticated key agreement and extends the results to Group –Diffie-Hellman key agreement. The paper presented new definitions and protocols geared for the dynamic peer group (DPG) settings. In particular, it showed how important security services (Key authentication, Key confirmation, and entity authentication. GDH.3 is a key-agreement model aimed at minimizing computations by group members. It is quite likely that the protocols presented in the paper can be improved [1]. E Bresson et al. presented group Diffie-Hellman protocols for authenticated Key exchange (AKE) are designed to provide a pool of players with a shared secret key which may use to achieve some cryptographic goals like multicast message confidentiality or multicast data integrity. In AKE, each player is assured that no other player aside from the arbitrary pool of players can learn any information about the session key. This study provided major contribution to the solution of the group Diffie-Hellman key exchange problem. Addressed in detail in this paper were two security goals of the group Diffie-Hellman key exchange: the authenticated key exchange and mutual authentication. The work provided the first formal treatment of the authenticated group Diffie-Hellman key exchange problem [2]. Recently, J. Katz et al. proposed scalable protocols for authentication group key exchange. This work was originally motivated by the fact that no proof of security appears in the proceedings version; furthermore, subsequent work in this area implied that the Burmester -Desmedt protocol was "heuristic" and had not been proven secure. The proposed protocol ensured that players send every

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

message to all members of the group via point-to-point links [3]. In [4] proposed a very efficient and provably secure group key agreement well suited for unbalanced networks consisting of devices with strict power consumption restrictions and wireless gateways with less stringent restrictions. The study has focused on computing applications involving clusters of mobile devices. In addition, the main contribution in this work is a provably secure authenticated group key-exchange scheme based on public-key cryptography that can complement the WEP protocol. This protocol allows a set of heterogeneous mobile devices to form a secure group and to handle the continuous disappearing and reappearing of mobiles due to communication failure. Additionally, this protocol has been proved secure in the random oracle model under the computational Diffie-Hellman assumption. In [5] (2005), the authors focus on constant-round protocol well suited for a mobile environment and prove its security under the decisional Diffi-Hellman assumption. This protocol was an efficient group key agreement protocol well suited for wireless networks consisting of a cluster of mobile devices with limited computational resource and stationary server with sufficient computational power. The protocol achieved perfect forward secrecy and has been proven secure against an active adversary under the decisional Diffie-Hellman assumption. In addition the work has also modified the stand and security model to consider a stronger and more realistic adversary R. Barua et al. proposed and analyses a variant of Burmester-Desmedt group key agreement protocol (BD) and enhance it to dynamic setting where a set of users can leave or join the group at any time during protocol execution with updated keys. The authors incorporated authentication in the proposed protocol using digital signature with appropriate modifications in Katz-Yung compiler. This method has the ability to detect the presence of a corrupted group number, although they couldn't detect who among the group members are behaving improperly. The protocol is simple and elegant constant round group key agreement protocol using a ring structure of participants and enhances it to dynamic setting where a group of uses can leave and join. By extending the security model in a natural way, they are able to prove the security of the dynamic protocol and the signature schemes are secure. The join and leave algorithms of this protocol reduced most user's computation cost significantly over doing a key exchange from scratch by executing BD protocol [9]. Y. -W. Chen, et al. treated with authentication and key agreement protocol to streamline communication activities for a group of mobile stations (MSs) roaming from the same home network (HN) to a serving network (SN).However, the author has designed structure makes the process more smooth which is; when the first MS of a group visits, the SN performs full authentication with the concerned HN and therapy obtains authentication information for the MS and other members. As shall be seen shortly, the proposed method scheme is characterized by several strengths. First, the security level of the scheme is same with counterpart AKA protocols. Further, the scheme might speed up handover procedure if the HN distributes authentication data to neighboring SNs is likely to visit next. Moreover, the design is well applicable to any system accommodating remote authentication servers, such as TETRA network, and (WiMAX) network…et. In G-AKA scheme, every MS provides its identity when visiting an SN. To realize, a group-based AKA protocol comprised three procedures: group information setup, authentication distribution, and mutual authentication and key agreement. A group-based authentication and key agreement enable the serving network to authenticate other MSs of the same group; therefore G-AKA is able to reduce both authentication delay and signaling overhead within the core network above that it uses a shared GTK and data structure (Index Table) to authenticate these MS's. The authentication delays and signaling overhead between the serving network and home network are reduced with G-AKA scheme [18].

3. AUTHENTICATION GROUPS IN MOBILE EVIRONMENT

In 2006, J Kim et al. presented a new group key agreement protocol which allows a set of heterogeneous mobile devices in different cells to form a secure group. This protocol showed that is able to offer the desired properties including key authentication, perfect forward secrecy and known key secrecy for a practical key agreement protocol. The proposed protocol focused on the extended model of which participants are several base stations and mobile devices in different cells [6]. Meanwhile, based on the short signature scheme from bilinear pairing; R. Lu et al. proposed a new authenticated encryption protocol with perfect forward secrecy for mobile communication. In an authentication encryption protocol a sender may use his own private key and the specified receiver's public key to make a signature-cipher text for a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

message and send it to the specified receiver. Later, only the specified receiver has the ability to recover and verify the message simultaneously .This protocol not only satisfied the basic security requirements: confidentiality, integrity, authentication, and nonrepudiation, but also provided the perfect forward secrecy [7]. In 2007, authors proposed a group authentication protocol for mobile networks (mGAP). The mGAP predicts nodes' behavior and manages the authentication of mobile groups and individual nodes during roaming across administrative domains. The protocol design distributed the load between the mobile access points and the mobile nodes taking into account the mobile nodes' limited resources. The architecture of the protocol is depends on the capacity of the home domain to analyses the mobile entity's behavior and information registered in the domain database, and to predict the authentication needs according to the home domain (HD) policy . mGAP treats the mobile access point both as a support for the mobile group and as an individual node. The support of the mobile access point leads to faster authentication to be implemented, namely, the mobile access point re-authenticated at the visited domain will avoid individual re-authentication of each node in the roaming group. The proposed protocol used mobile access point and aims at the predicting the authentication profile of the mobile entities. The authentication profile can be updated in case of unexpected changes, while keeping the possibility of authentication by proxy to the home domain, whenever needed. mGAP is based on new cryptographic primitive (group encryption) that is used for the first time in mobile networks; this primitive allows for a flexible and scalable authentication process over different administrative domains [8]. C. -C. Lee et al. tried to present a new authenticated group key agreement to remedy it. It is based on bilinear pairing. The proposed protocol focused on a secure contributory group key agreement. A secure group key agreement protocol design for mobile wireless network is an important issue to provide secure services among mobile devices. The protocol has proposed to ensure the validity of the transmitted messages. The security of this presented protocol is based on solving BDLP and BCDHP in bilinear pairing, and also can apply to asymmetric mobile environment. That is, the protocol participants consist of a stationary sever and a cluster of mobile devices [11]. In [13] introduced an anonymous batch authentication and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time. ABAKA can efficiently authenticate session key with each vehicle by one broadcast message. The security of ABAKA is based on the elliptic curve discrete logarithm problem, which is an unsolved NP-complete problem. The paper has demonstrated the efficiency merits of ABAKA through performance evaluations in terms of verification delay, transmission overhead, and cost for re-batch verifications, respectively. The current scheme achieved mutual authentication between the SP and requesting vehicles based on ECDLP and ECDSA certificates, session key establishment, privacy preservation, and low transmutation overhead and fast verification. Furthermore, the proposed scheme is to build a secure environment for value-added service in VANETs. With ABAKA, scheme an SP can simultaneously authenticate multiple requests and establish different session keys with vehicles. ABAKA considers not only scalability and security issues but privacy preserving as well.

4. AUTHENTICATION IN MACHINE TYPE COMMUNICATIONS

Zhang et al. exhibited a Dynamic Group Based Authentication Protocol for MTC and essential agreement (DGB-AKA) for MTC communication. Be that as it may, in this co-found group, each MTC device Pre-offer an extra secret key with the home environment and other MTC devices have a place in the same collection. Moreover, which it is comparable with SE-AKA, the principal MTCD performs a full confirmation with the home environment, the rest MTCDs of this collection only authentication with aiding network. The technique for group key upgrade has proposed to be suited for dynamic MTC bunch. Additionally, to bolster dynamic determination of group header and adaptive of group size, and diminish the multifaceted nature of MTC group update [16]. C Lai et al. follow Zhang and presented a novel group access authentication and key agreement protocol for machine type communication to reduce authentication signaling costs and network access latency and to efficiency authentication MTC devices of the same group. In this proposed protocol, the first MTC devices accessing the network performs a full authentication and key agreement authentication procedure and obtains a group temporary key and group authentication information on behalf of other MTC devices in the same group; then, the remaining MTC devices perform a simplified authentication procedure

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

locally. A novel group access AKA protocol for MTC, called MTC-AKA, to facilitate MTC devices, which have been subscribed in the HN to roam from HN to SN. In the MTC-AKA, each MTC devices provides its identity when it visits an SN. Assisted by the HN, the SN examines whether the MTC device belongs to a group, and completes a full authentication procedure for the first MTC devices in a group. In conclusion, the MTC-AKA is able to provide a simple and security authentication procedure, a robust key exchange process and several security features, and it requires less bandwidth consumption, fewer signaling messages between the HN and the SN and smaller storage space in the SN compared with the conventional schemes on performance [20]. On the same concept, R- Jaing et al. proposed a group authentication and key agreement protocol, called EG-AKA, for machine-type communication combining elliptic curve Diffie-Hellman (ECDH) based on EAP framework. This protocol guaranteed stronger security and provides better performance. In this technology, the group is assigned a unique identifier, and user terminals are authenticated together as corporate entities. Group authentication can be fulfilled by utilizing the authentication agency or the gateway. After successful group authentication, users terminals and networks side entities can share some keys. Moreover, in order to achieve the proposed group authentication protocol, there are three phases in the proposed protocol: group initialization, authentication data distribution, and mutual authentication and key agreement. The main aim in this protocol is to handle specific group access authentication for non-3GPP MTC. The proposed EG-AKA protocol not only enhances security on the basis of Mun's protocol, but also designs specific group authentication mechanism for MTC. Detailed evaluations of performance illustrated that proposed protocol achieved better performance in terms of transmission and signaling overhead [21]. As of late, Lai et al. (2014) likewise proposed a Secure and Efficient Group individuals and powerful group wandering scheme for MTC somewhere around 3GPP and WiMAX Networks, which name SEGR. Additionally, this scheme described by confirming all MTC gadgets in a set at the same time and accelerating the procedure of handover authentication by receiving a certificate less aggregate signature. Also, the entrance system can at the same time trust a group of MTC gadgets and create free session key with each MTC gadgets. Besides, this proposed that be SEGR scheme it was the first to target secure and efficient 3GPP-WiMAX wandering performed by the group [22]. Y. Zhang et al. in [2014] provided a group-based authentication and key agreement for MTC communications. Besides a secret key shared between Serving Network (SN) and Home Environment (HE), each member also shares a group key with (HE) and other members of the group. This paper presented a dynamic group-based authentication and key agreement (DGBAKA) for MTC communication. In this co-located group, each MTC devices pre-shares and additional secret key with home environment and the other MTC devices belong to the same group. The key will be shared for authenticating with serving network locally. The redundant signaling could be eliminated to avoid congestion by a shared group authentication key. Also the link resource between SN and HE could be saved by using the shared arrays of authentication vector when the number of MTC devices is large. DGBAKA protocol could solve the problem of the congestion and overload caused by co-located MTC group roaming. In the scheme, all of the devices belonging to the same group share a key with HE for authentication. Thus, these devices could use the same array of authentication vectors and only one of these devices needs a full AKA interaction with HE firstly, while the others locally authenticate with SGSN [25].

5. AUTHENTICATION GROUPS IN LTE NETWORKS

A batch authentication and key agreement for LTE networks is proposed in this paper by W. Zhang et al. based on an improved GAA architecture to achieve end-to-end security in application layer. In this protocol, the application server aggregates received group authentication request massages, and then delivers it to BSF for verification. Subsequently, the mutual authentication and key agreement between the NAF and each UE achieved. The program can shorten the authentication delay, reduced network congestion, allow mobile service providers to focus on mobile business, and end to end security applications covered by the application can provided by unified operator platform [33].

6. AUTHENTICATION GROUPS PROTOCOLS FOR MACHINE-TYPE COMMUNICATION IN LTE NETWORKS

Jin Cao and his colleagues attempted to comprehend serious signaling in Long Term Evolution (LTE) by displaying a group- based access authentication scheme. It is made the MTC devices ready to get confirmation at the same time

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by the framework and build up a free session key with the system independently. Moreover, it takes aggregate signature in which a group pioneer of MTC gadgets and sends the aggregate signature to the Mobility Management Entity (MME), and then MME can successfully and rapidly verify an arrangement of MTC devices. In any case, its computational overhead is moderately significant because it takes bilinear pairing and Elliptic Curve algorithm technique [15]. In 2010, K. -R. Jung, proposed a new congestion avoidance algorithm to reduce the congestion of the uplink intensive application. Proposed congestion avoidance method is co-operation manipulation and report method for aggressive MTC sensor device environments. In this method, MTC devices are metering devices, and transfer metered information to the MTC server periodically. In this article, they analyzed the state of the art of the machine type communication in mobile broadband communication domain, especially for 3GPP standardization issues. In conclude, the proposed method reduces the network load at uplink by using a grouping method at dense area local network [12]. Lai, Chengzhe, Li Hui, Rongxing Lu, Jiang Rong. Proposed a lightweight Group authentication protocol for MTC in the Long-Term Evolution systems again, called LGTH. LGTH receives a total signature in light of message authentication codes, and it is can verification a group of MTC Devices rapidly and all the while. Also, a significant number of devices getting to the system at the same time that is the reason for separate verification signaling congestion. Additionally, this strategy attempted to take care of the issue that is lessening authentication overhead of the past plans given public key cryptosystem. Also, LGTH has a little computation and communication costs, however, it cannot provide security insurance [19] [2013]. In [32], scholars presented a group-based access authentication scheme, by which a good deal of MTC devices can be simultaneously authenticated by the network and establish an independent devices to the network respectively. Proposed scheme not only greatly reduce the signal transmission for mass of devices to the network and thus avoid the signaling overload over LTE network but also achieved robust security including key forward/backward secrecy and non-repudiation verification. In this protocol not only mutual authentication and key agreement between each MTCD in a group and the mobile management entity (MME) has achieved but, also can greatly reduce the signaling traffic and thus avoid network congestion. Furthermore, the GBAAM scheme can resist the several existing attacks and achieve robust security protection including KFS/KBS and non-repudiation verification.

7. AUTHENTICATION GROUPS PROTOCOLS FOR MACHINE-TYPE COMMUNICATION IN LTE-ADVANCED NETWORKS

In this field J. Cao et al. abled to gather and proposed a productive group based anonymity handover confirmation protocol for a large number of MTC gadgets with mobility [26]. Furthermore, the paper has considered the first group based handover authentication strategy in LTE-A systems. The scheme has been able to do to a great extent decreasing the signaling expenses and the correspondence costs in both access system and the center system and guaranteeing client's protection [2015]. In addition, Cao et al. displayed a Uniform Group –based Handover Authentication Protocol for MTC inside E-URAN in LTE-A systems. Be that as it may, when the MTC bunch moves to the objective eNB, the objective eNB can confirm a collection of MTC devices by checking the multi-signature. Moreover, in the mobile MTC application supporting the LTE-A system, the regular handover signaling connections not just purpose the signal loads on the systems hubs; additionally, build the terminal vitality utilization. Likewise, this proposed has demonstrated that UGHA can give a straightforward verification process with strong security assurance, diminish the signaling expenses, and abstain from signaling congestion [29]. Afterthought, Choi et al. Proposed design of an efficient security protocol for MTC. This protocol is designed to be compatible with the incumbent system by being composed of only symmetric cryptography. However, the concentration of this paper is when a group of devices attempt to register simultaneously , masses of signalling traffic associated with AKA would generate significant overloads on the authentication server create bottleneck in the link between a server and devices. To avoid that the authors has emphasized the need for the design of an efficient AKA procedure that reduces repetitive invocation of costly authentication signalling, especially in situation of group optimization. Moreover, this paper has objected to take significant steps toward a new security mechanism that reduces the volume of signalling traffic in the AKA phase, even if the number of MTC devices is large and variable. In the proposed protocol the leader in the group holds the responsibility for mutual authentication and secure key distribution and takes an advantage of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the batch verification to save communication overhead and computational overhead. The leader collect authentication requests from MTC devices through this channel and compresses them into a signal request. The proposed protocol comprised four phases: system initialization, mutual authentication, membership update, and session key agreement. The mechanism improved grouping optimization by aggregating authentication requests and uses Wi-Fi hotspots as a secondary channel to share data among devices and also able to be extended to make use of more advanced access network, such as multi hops and D2D [27]. Another paper proposed in 2015 by H. Choi and his friends to enhance security overheads in the radio access network by utilizing group-based authentication. The proposed method has presented as part of a security remedy, a group-based authentication and key agreement. This proposal leverages group information to simultaneously authenticate each group member and, as a result, alleviates congestion in the control plane and overhead in the radio link generated from a group of MTC devices. The G-AKA ensured many properties such as the mutual authentication between MTC devices and the MME via a challenge-response protocol, and confidentiality and integrity key agreement. At that time G-AKA considered better than the traditional LTE-AKA in terms of handshake overhead if the number of group members is greater than two. Furthermore, the development of 3GPP M2M communication is in its infancy, and its development further raises numerous security issues that deserve investigation. As a part of a security remedy in MTC security, we envisioned a group-based authentication and key agreement that operates by leveraging group information to authenticate a number of devices in a group efficiently and effectively without any need of excessive authentication signalling [31]. By following the strategy J. LI and others presented a group-based AKA (GR-AKA) protocol with dynamic policy updating. The authors has chosen an asynchronous secret share scheme combining with Diffie -Hellman key exchange scheme to implement distributed authentication and session key establishment in the LTE-A networks, and to achieve dynamic MTC-devices access authority updating. However, if a large number of devices request to access the network during a short period, users will suffer from high network access latency and authentication signalling congestion. This is because every device has to perform a full AKA authentication procedure, which will rapidly increase the authentication vectors generated by home authentication sever. The authors have proposed a solution for this problem which is group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. Moreover, the main contributions of the article are: GR-AKA provides a group authentication mechanism, which could efficiently and simultaneously authentication multiple MTCDs. Compared with other asymmetric cryptography-based authentication such as EPS-AKA, GR-AKA reduces the transmission overhead in the LTE-A network and decrease the computation overhead in the operator domain. The second contribution that is GR-AKA has enabled the MTC system to update the access policy of MTC devices. Comparing with existing authentication groups GR-AKA has achieved the updating with responsible computation and storage overhead. The GR-AKA provided strong security properties, achieved security requirement mention in prior AKA protocols, above that, proposed method enables the system to dynamically update its access-policy in an efficient way. Furthermore, the bandwidth consumption of GR-AKA is much lower than that of UTMS-AKA and EPS-AKA, and is better than other protocols (S-AKA, G-AKA, SE-AKA, and CAO-AKA) when the HN is located far from SN [28].

8. AUTHENTICATION WITH PRIVACY-PRESERVING IN MTC AND MOBILE COMMUNICATIONS

With missing the privacy of mobile communication in 2008 R Lu et al. introduced efficient conditional privacy preservation (ECPP) protocol in vehicular ad hoc networks (VANETs) to address the issue on anonymous authentication for safety message with authority traceability. The proposed protocol is characterized by the generation of on-the-fly short time anonymous keys between on-board units (OBUs) and roadside units (RSUs), which can provide fast anonymous authentication and privacy tracking. The ECPP protocol can efficiently deal with the growing revocation list while achieving conditional traceability by the authorities. The proposed protocol (ECPP) has been identified to be not only capable of providing the conditional privacy preservation that is critically demanded in the VANETs application, but also able to improve efficiency in terms of the minimized anonymous keys storage at each OBU, fast verification on safety message, and an efficient conditional privacy tracking mechanism [10]. Fu et al. (2012) exhibited

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

a Novel Group-Based handover authentication scheme for overall portable interoperability for microwave access (WiMAX) systems. Moreover, when the first mobile station moves from the administration base station (BS) to an objective BS, the administration BS transmits all the handover group members' security context to the real BS. Additionally, whatever remains of MSs of this group can straightforwardly perform handover authentication. Moreover, this proposed not just meets the vital security necessities in handover authentication semantics, (for example, Mutual authentication and opposing the domino impact) additionally accomplished a piece of privacy preservation [17]. By focusing on his interesting area which is achieve the privacy preserving in different platforms A. Fu and his supporters presented a privacy preserving fast handover authentication scheme based on pseudonym for IEEE 802.16m network. Since mobile stations (MS) only provides a pseudonym in the initial authentication phase and change its pseudonym in each handover authentication phase, this can protect the MS's identity privacy and allow MS to be untraceable. The proposed scheme not only fulfils the essential handover security requirements but also achieves privacy preserving. The presented work does not require MS to perform any complicated operation, which is well suited for limited-power MS in wireless network [14]. In 2015, J. Sun et al. proposed two novel privacy-preserving spatiotemporal matching protocols. The work tackles this open challenge and proposes spatiotemporal matching as a promising enabler for secure D2D communication. This approach, however, does not permit the initiating user to further distinguish potentially many candidates having a valid certificate. This technique is motivated by the fact that almost all target D2D devices are location-aware through cellular, Wi-Fi, or GPS technology. The study contained three contributions. First, it has coined privacy-preserving spatiotemporal matching as a fundamental primitive for secure D@D communication. Second, it is presented two solutions towards efficient privacy-preserving spatiotemporal matching. The first solution is a passive approach, in which every mobile user periodically records his locations, and user's spatiotemporal profile is defined as a set of (time, location) pairs. The second solution is an active approach, where every mobile user continuously broadcasts cryptographic tokens and also records every token he overhears. The third contribution, the method proposed two protocols for the privacy-preserving comparison of two arbitrary active/passive spatiotemporal profiles. A novel privacy-preserving spatiotemporal matching protocol and a novel weighted privacy-preserving spatiotemporal matching protocol based on a novel use of the Bloom filter [35].

9. AUTHENTICATION WITH PRIVACY-PRESERVING FOR MTC IN LTE/LTE-A NETWORKS

In 2016 A. Fu, could proposed a Privacy-Preserving Group Authentication Protocol for MTC in LTE/LTE-Advanced systems. Be that as it may, the proposition accomplished to get validates all the while with a set of MTCDs by receiving Pairing-Free personality based cryptography and complete message authentication code. Moreover, it can channel some illicit MTCDs by confirming MACG1 in the fourth methodology of mutual authentication, in this way it might proficiently maintain a strategic distance from Denial of services (DoS) attacks. Also, the scheme gives robust privacy preserving including client secrecy and traceability. Additionally, it keeps away from congestion avoidance and mutual authentication. Subsequently, it minimizes the signaling congestion and calculation overhead.

10. CONCLUSION

In summary, we present a groups authentication and the techniques that used to improve the authentication process and robust the privacy-preserving for machine type communication (MTC) in LTE/LTE-A networks. Our point is to select the most efficient group has reduced the signalling overhead and computational. Moreover, the paper has covered all the work that tried to enhance the core network and get rid of the congestion signalling.

REFRENCES:

[1] G. Ateniese, M. Steiner, and G. Tsudik, "New Multiparty Authentication Services and Key Agreement Protocols," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 628–639, 2000.

[2] E. Bresson and D. P. J. Quisquater, "Provably Authenticated Group Diffie-Hellman Key Exchange," Comput. Commun. Secur., vol. 01, no. 7, pp. 255–264, 2001.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] J. Katz and M. Yung, "Scalable Protocols for Authenticated Group Key," Adv. Cryptology-CRYPTO 2003, vol. 2729, no. 4, pp. 110–125, 2003.

[4] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices *," Comput. Commun., vol. 27, no. 17, pp. 1730–1737, 2004.

[5] J. Nam, J. Lee, S. Kim, and D. Won, "DDH-based group key agreement in a mobile environment," J. Syst. Softw., vol. 78, no. 1, pp. 73–83, 2005.

[6] J. Kim, S. Kim, K. Chun, J. Lee, and D. Won, "Group Key Agreement Protocol Among Mobile Devices in Different Cells," Springer Berline Heidelb., vol. 4331, no. 9, pp. 1090–1097, 2006.

[7] R. Lu, Z. Cao, and X. Dong, "Authenticated encryption protocol with perfect forward secrecy for mobile communication," Wirel. Commun. Mob. Comput., vol. 6, no. 3, pp. 273–280, 2006.

[8] N. Aboudagga and J. Quisquater, "Group Authentication Protocol for Mobile Networks," Netw. Commun., no. WiMob, 2007.

[9] R. Dutta and R. Barua, "Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007–2025, 2008.

[10] R. Lu, X. Lin, H. Zhu, P. Ho, and X. S. Shen, "ECPP : Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," Comput. Commun., vol. 6, no. 7, pp. 1903–1911, 2008.

[11] C. L. T. Lin and C. Tsai, "A new authenticated group key agreement in a mobile environment," Ann. Telecommun., vol. 71, no. 483, pp. 735–744, 2009.

[12] K. Jung, A. Park, and S. Lee, "Machine-Type-Communication (MTC) Device Grouping Algorithm for Congestion Avoidance of MTC Oriented LTE Network," Commun. Comput. Inf. Sci., vol. 78, no. 7, pp. 167–178, 2010.

[13] J. Huang, L. Yeh, and H. Chien, "ABAKA : An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, 2011.

[14] A. Fu, Y. Zhang, Z. Zhu, Q. Jing, and J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802 . 16m network," Jouranl Comput. Secur., vol. 31, no. 6, pp. 741–749, 2012.

[15] L. H. Cao, Jin, Ma Maode, "A Group-based Authentication and Key Agreement for MTC in L TE Networks," J. Commun. Inf. Syst. Secur. Symp., pp. 1017–1022, 2012.

[16] Y. Zhang, J. Chen, H. Li, W. Zhang, J. Cao, and C. Lai, "Dynamic Group based Authentication Protocol for Machine Type Communications," Intell. Netw. Collab. Syst. (INCoS), 2012 4th Int. Conf., 2012.

[17] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, "A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks," IEEE Commun. Lett., vol. 16, no. 11, pp. 1744–1747, 2012.

[18] Y. C. J. W. K. Chi and C. Tseng, "Group-Based Authentication and Key Agreement," Wirel. Pers. Commun., vol. 62, no. 4, pp. 965–979, 2012.

[19] J. R. Lai, Chengzhe , Li Hui, Rongxing Lu, "LGTH : A Lightweight Group Authentication Protocol for Machine-Type Communication in LTE Networks," J. Commun. Inf. Syst. Secur. Symp. LGTH, vol. 16, no. 2, pp. 832–837, 2013.

[20] C. Lai, H. Li, X. Li, and J. Cao, "RESEARCH ARTICLE A novel group access authentication and key agreement protocol for machine-type communication," Emerg. Telecommun. Technol., vol. 26, no. 3, pp. 414–431, 2013.

[21] R. Jiang, C. Lai, J. Luo, X. Wang, and H. Wang, "EAP-Based Group Authentication and Key Agreement Protocol for Machine-Type Communications," Int. J. Distrib. Sens. Networks, vol. 2013, no. 99, p. 14, 2013.

[22] Lai, Chengzhe , Li Hui, Rongxing Lu , Jiang Rong, "SEGR : A Secure and Efficient Group Roaming Scheme for Machine to Machine Communications between 3GPP and WiMAX Networks," J. Commun. Inf. Syst. Secur. Symp., pp. 1011–1016, 2014.

[23] S. M. Evice, T. O. Mart, M. Alam, D. Yang, J. Rodriguez, and R. A. Abd-alhameed, "Secure Device-to-Device Communication in LTE-A," no. April, pp. 66–73, 2014.

[24] T. Taleb, S. Member, A. Ksentini, and S. Member, "Lightweight Mobile Core Networks for Machine Type Communications," Jouranl IEEE Access, vol. 2, 2014.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[25] U. Computing, "Group-based authentication and key agreement for machine-type communication Yueyu Zhang *, Jie Chen , Hui Li , Jin Cao and Chenzhe Lai," Int. J. Grid Util. Comput., vol. 5, no. 2, pp. 19–21, 2014.

[26] J. Cao, H. Li, and M. Ma, "GAHAP : A Group-based Anonymity Handover Authentication Protocol for MTC in LTE-A Networks," Mob. Wirel. Netw. Symp., pp. 3020–3025, 2015.

[27] S. Choi, Daesung , Hong, "A Group-based Security Protocol for Machine Type Communications in LTE-Advanced," J. Mob. Commun. Comput. Inf., vol. 21, no. 2, pp. 161–162, 2015.

[28] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A Networks," IEEE Internet Things J., vol. 3, no. 3, 2015.

[29] J. Cao, H. Li, M. Ma, and F. Li, "UGHA : Uniform Group-based Handover Authentication for MTC within E-UTRAN in LTE-A Networks," J. 2015 IEEE Int. Conf. Commun., pp. 7246–7251, 2015.

[30] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A Two Level Privacy Preserving Pseudonymous Authentication Protocol for VANET," J. Wirel. Mob. Comput. Netw. Commun. (WiMob), vol. 4, no. 10, pp. 643–650, 2015.

[31] H. Choi, "Improvement of Security Protocol for Machine Type Communications in LTE-Advanced," Wirel. Commun. Mob. Comput., vol. 66, no. 9, pp. 1301–1306, 2015.

[32] J. Cao, M. Ma, and H. Li, "RESEARCH ARTICLE GBAAM : group-based access authentication for MTC in LTE networks," Secur. Commun. Networks, vol. 8, no. 17, pp. 3282–3299, 2015.

[33] W. Zhang and X. Wang, "A GAA-based batch authentication and key agreement for LTE networks Yunya Zhou Yumin Wang," Int. J. Embed. Syst., vol. 7, no. 3–4, pp. 289–295, 2015.

[34]A. Fu, J. Song, S. Li, G. Zhang, and Y. Zhang, "A privacy-preserving group authentication protocol for machine-type communication in LTE / LTE-A networks," J. Secur. Commun. Networks, vol. 9, no. 13, 2016.

[35] V. Odelu, A. K. Das, and A. Goswami, "SEAP : Secure and Efficient Authentication Protocol for NFC Applications Using Pseudonyms," Jouranl 30 IEEE Trans. Consum. Electron., vol. 62, no. 1, pp. 30–38, 2016.

[36] J. Sun, S. Member, R. Zhang, Y. Zhang, and S. Member, "Privacy-Preserving Spatiotemporal Matching for Secure Device-to-Device Communications," IEEE Internet Things J., vol. PP, no. 99, pp. 1–13, 2016.