ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Accomplish Secure Handover Session Key Management through Portable Relay in LTE Advanced Networks

S.Saran Kumar[1], T.Ranjith[2], V.Bharath[3], J.Sathiya Jeba Sundar[4]

UG Student, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1,2,3]

Assistant Professor, Velammal Institute of Technology, Chennai, Tamil Nadu, India [4]

ABSTRACT: Long Term Evolution, It increases the capacity and speed using a different radio interface together with core network improvements.To decrease the correspondence overhead and the computational unpredictability, a novel intermediary re-encryption method is utilized, where the session keys at first scrambled with the general population key of the portability administration substance (MME) will be re-scrambled by a portable transfer hub (MRN), with the goal that different DeNBs can later unscramble the session keys with their own private keys while without the coordinate inclusion of the MME.Point by point security investigation appears that the proposed plan can effectively build up session keys between the on-board UEs and their associated DeNB, accomplishing in reverse and forward key partitions, and opposing against the conspiracy between the MRN and the DeNB as a similar time.Internet of Things (IoT) is growing the system by coordinating immense measure of encompassing articles which requires the safe and dependable transmission of the high volume information era, and the versatile transfer procedure is one of effective ways to meet the on-board information blast in LTE-Advanced (LTE-A) systems.

KEYWORDS: Long Term Evolution,Machine Type Communication,Secure and Efficient Data Transmission,Wireleass Sensor Network,Data Security,Mobile Relay.

I. INTRODUCTION

With the accelerating growth of context-aware applications, the device-to-device (D2D) communication playsan important underlay role over the cellular network [1]. However, D2D communication cannot be realized without an efficient D2D discovery scheme, which involves nearby users (UEs) to search for the proximity-based service. Despite its importance, relatively less attention and research have been addressed to D2D discovery.Generally speaking, a pair of UEs moving within close proximity to each other in an LTE-A network, can establish a D2D link with or without the assistance of the serving eNB(s) [2]. More specifically, the D2D discovery scheme can be divided into two types: network-assisted and direct discovery [3]. The network-assisted D2D discovery requires the D2D UE connected to the BS all the time, which leads to inefficient use of network resource, large battery consumption, and the challenging of stability. On the contrary, the direct D2D discovery relies on the abilities of the D2D UEs to autonomously discover other D2D UEs. The BS only periodically broadcasts the available resources for transmitting and receiving discovery beacons, by which the energy and signaling overhead at the BS can be hugely reduced. Moreover,the direct D2D discovery has been employed in experimental prototypes [4]. In this paper, we focus on the performance of the direct D2D discovery in LTE-A networks.

For the network-assisted D2D discovery, a social-awareD2D discovery scheme underlying cellular networks was proposedin [5], where each group of D2D UEs is allocated theoptimal beacons probing rate with constant intervals. However,social network characteristics (such as real human mobilitytraces) are difficult to be acquired. Moreover, the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

D2D UEs aretypically power-limited, which means the energy-consumingD2D discovery scheme is not suitable for such problem.

II. LITERATURE REVIEW

In 2016,Nina Lin, Xiujie Huang and Xiao Ma had published"*Analysis of the Uplink Capacity in the High-speed Train WirelessCommunication with Full-duplex Mobile Relay*".One primary challenge in the high-speed train (HST) communication is that the wireless signal suffers from severe attenuation while it penetrates the sealed carriage of the train. In this letter, we show that such a nuisance can provide an opportunity of improving the uplink capacity when a full-duplex (FD) mobile relay (MR) is furnished on the train. To this end, by introducing the self-interference cancellation (SIC) level, we present an uplink channel model for the HST communication with FD MR. Then the uplink capacity is analyzed under either user equipment power constraint or total power constraint. By comparing with time division scheme, we can derive the required SIC level for the FD scheme to bring capacity improvement, which is confirmed by numerical results. Furthermore, theoretical analysis shows that, for a given SIC level, the uplink channel with severer carriage attenuation has higher capacity, which is also validated by numerical results.

In 2015**,**Zhenyu Zhou,Mianxiong Dong, Kaoru Ota,GuojunWang had published a "*Energy-Efficient Resource Allocation for D2D Communications Underlaying Cloud-RAN based LTE-A Networks*".Device-to-device (D2D) communication is a key enabler to facilitate the realization of the Internet of Things (IoT). In this paper, we study the deployment of D2D communications as an underlay to long-term evolution-advanced (LTE-A) networks based on novel architectures such as cloud radio access network (C-RAN). The challenge is that both energy efficiency (EE) and quality of service (QoS) are severely degraded by the strong intracell and intercell interference due to dense deployment and spectrum reuse. To tackle this problem, we propose an energy-efficient resource allocation algorithm through joint channel selection and power allocation design. The proposed algorithm has a hybrid structure that exploits the hybrid architecture of C-RAN: distributed remote radio heads (RRHs) and centralized baseband unit (BBU) pool. The distributed resource allocation problem is modeled as a noncooperative game, and each player optimizes its EE individually with the aid of distributed RRHs. We transform the nonconvex optimization problem into a convex one by applying constraint relaxation and nonlinear fractional programming.

In 2014,Chan-Kyu Han, Hyoung -Kee Choi had published"*Security Analysis of Handover Key Management in 4G LTE/SAE Network*".The goal of 3GPP Long Term Evolution/System Architecture Evolution (LTE/SAE) is to move mobile cellular wireless technology into its fourth generation. One of the unique challenges of fourth-generation technology is how to close a security gap through which a single compromised or malicious device can jeopardize an entire mobile network because of the open nature of these networks. To meet this challenge, handover key management in the 3GPP LTE/SAE has been designed to revoke any compromised key(s) and as a consequence isolate corrupted network devices. This paper, however, identifies and details the vulnerability of this handover key management to what are called desynchronization attacks; such attacks jeopardize secure communication between users and mobile networks. Although periodic updates of the root key are an integral part of handover key management, our work here emphasizes how essential these updates are to minimizing the effect of desynchronization attacks that, as of now, cannot be effectively prevented.

In 2014,Chengzhe Lai, Hui Li, Rongxing Lu, Rong Jiang, and Xuemin (Sherman) Shen had published"*SEGR: A Secure and Efficient Group Roaming Scheme for Machine to Machine Communications between 3GPP and WiMAX Networks*".With extensive promising applications, machine to machine (M2M) communications or machine-type communication (MTC) have attached a tremendous interest among mobile network operators and research groups. Supporting multiple MTC devices has been considered as an essential requirement in M2M communications.

In 2012,LucaCostantino,NovellaBuonaccorsi,ClaudioCicconetti, RaffaellaMambrini had published" *Performance Analysis of an LTE Gateway for the IoT*". In the Internet of Things (IoT) the edge devices often rely on gateways to

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

connect to the Internet, to reduce costs and energy consumption. For those scenarios where the gateway itself does not have a wired Internet connection, LTE is a candidate solution due to its high spectral efficiency, bandwidth, and coverage. In this paper, the suitability of LTE for the interconnection of aggregated edge devices is investigated. The study is carried out under the assumption that the Constrained Application Protocol (CoAP), which is becoming increasingly popular, is used. The performance analysis is carried out through packet-level simulation with the open source simulator ns3.

III.PROPOSED SYSTEM

We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SETIBOOS, by using the IBS scheme and the IBOOS scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto-systems.We devise a novel secure handover key management scheme inLTE-A networks, when the MRNs are owned by third parties.With the proposed handover key management scheme, each on-board UE can successfully establish its session key with the DeNB during the handover process while guaranteeing the forward and backward session key separations.We propose our handover key management in MRN scenario, followed by security analysis and performance evaluation.

➢ System design

The mobile relay network scenario under the 3GPP LTE architecture is composed of the access domain (Evolved Universal Terrestrial Radio Network, E-UTRAN) and the core domain (Evolved Packet Core, EPC) [20]. The access domain consists of on-board UEs, MRNs installed on public transportation, and mobile relay capable DeNBs, as shown in Fig. 1. The DeNBs are connected to each other through the X2 link, while the DeNB and the MME is connected by the S1-C link [20]. When public vehicles or trains are moving forward, the UEs located inside the carriage maintain their connections to the network by communicating with the MRNs which are moving along with the on-board UEs. While at the same time, the MRNs communicate with the fixed DeNBs located near the roads or railways. In the core network domain, we only take the mobility management entity (MME) into consideration, and the functionalities of an MME includes performing mutual authentication with the UEs on behalf of the EPC and taking control of mobility management of the Ues.When an on-board UE communicates with one DeNB through the cooperation of a MRN, it may roam out of the coverage area of the current DeNB, and then connect to another DeNB. The 3GPP LTE network supports two types of handover, i.e., inter-MME handover and intra-MME handover. Since the inter-MME handover occurs between the UE and MME by running full Evolved Packet System authentication key agreement (EPS-AKA) procedure, without the involvement of any signaling transmission between DeNBs, we only consider the intra-MME handover process and focus on the wireless links between the DeNB and the on-board UEs. Under this mobile relay network scenario, the on-board UEs conduct intra-MME handover between two neighboring DeNBs with the help of a MRN which is moving along. When a group of on-board UEs roam to the coverage of a new DeNB, new session keys need to be generated and established to protect the security of the radio access links between the on-board UEs and the new DeNB.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

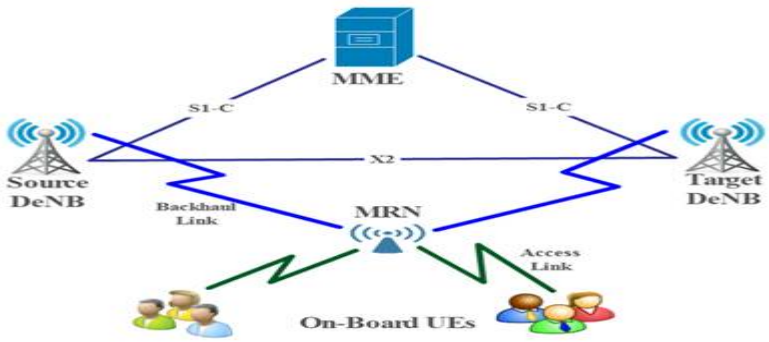

FIGURE 1.0

A. NETWORK CONFIGURE

This module creates network structure such as server, client and some intermediate nodes. All Nodes are inter connected like wireless sensor network. A wireless sensor network (WSN) of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

B. HYPER SPLIT

To fill the gap between theory and practice, in this paper, we propose a novel packet classification algorithm named Hyper Split. Compared to the well-known HiCuts and HSM algorithms, HyperSplit achieves superior performance in terms of classification speed, memory usage and preprocessing time. The practicability of the proposed algorithm is manifested by two facts in our test: HyperSplit is the only algorithm that can successfully handle all the rule sets.

C. SECURE ANALYSIS

To send files from source to destination, files are converted to full secure format. Here we implement security to base on AES encryption algorithm and DSA algorithm. Key generation has two phases. The first phase is choice of *algorithm parameters* which may be shared between different users of the system, while the second phase computes public and private keys for a single user. Each packet has a key to implement more security.

D. REPUTATION OVER NETWORK

Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems - data aggregation and data trustworthiness assessment - using a single iterative procedure. Such trustworthiness estimate of each sensor is based on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is usually a weighted average; sensors whose readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round of iteration their readings are given a lower weight.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

E. NODE AGGREGATION

Before the file reaches the destination node, grouping is done by combining all split data into one file using clustering methods. The receiver receives the file after decrypting the file using DSA key and displays the original files. Receiver also shows how many attackers have tried attack the file and checks the router names.

F. PERFORMANCE MEASUREMENT

The performance measurement tracks the speed of file transfer, efficiency and generates report about node connectivity details. This allow us to check how many files has been transferred and in which nodes it has been transferred efficiently.

➢ PROPOSED ALGORITHM

HyperSplit achieves superior performance in terms of classification speed, memory usage and preprocessing time. The practicability of the proposed algorithm is manifested by two facts in our test: HyperSplit is the only algorithm that can successfully handle all the rule sets; HyperSplit is also the only algorithm that reaches more than 6Gbps throughput on the Octeon3860 multi-core platform when tested with 64-byte Ethernet packets against 10K ACL rules.

IV. RESULTS

FIGURE 1.1- SERVER AND CLIENT STATUS

Initially the server and the router are disabled. Once any of the router is enabled, the server status will be visible.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

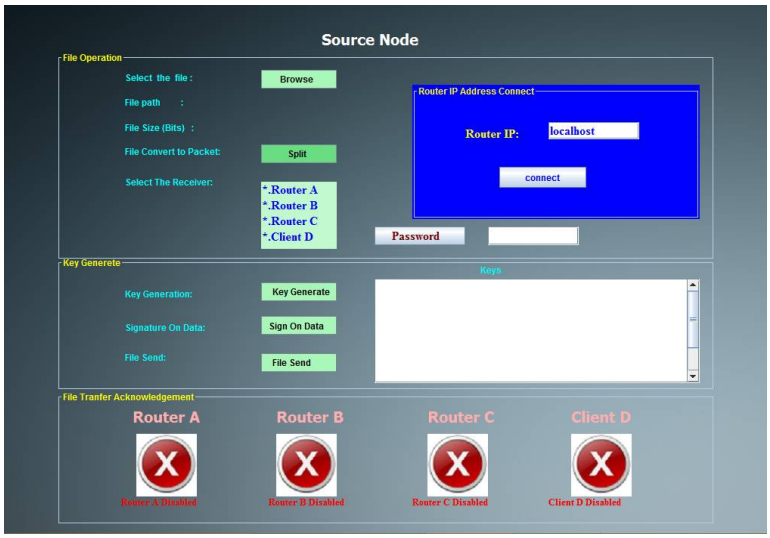

FIGURE 1.2-GENERATING ROUTER IP ADDRES

In order to enable the router, provide the router IP address and click on to connect.

FIGURE 1.3-ROUTER IP ADDRESS CONNECTION

Provide the same IP address and the password in this login page and click on connect.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

FIGURE 1.4-ENABLED ROUTER A

As the local host has been connected, the router A under the particular server has been enabled.

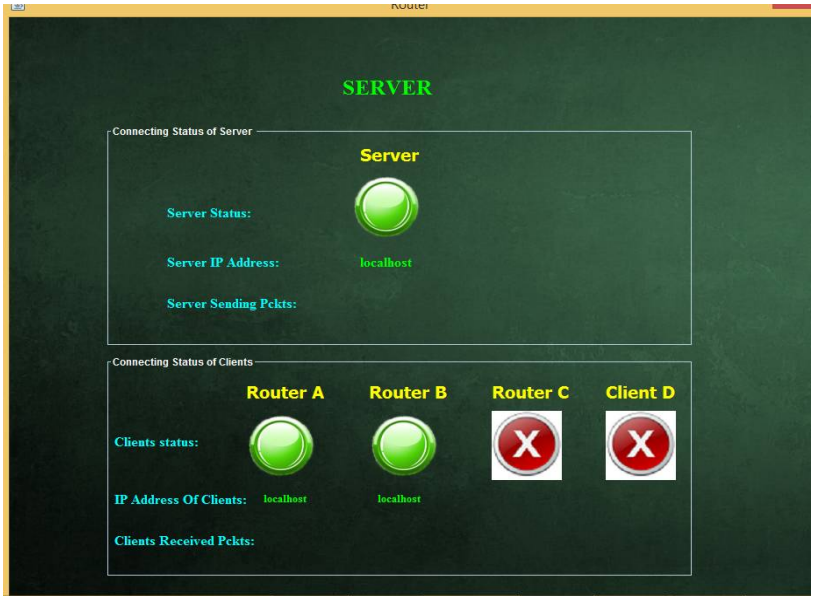

FIGURE 1.5-ENABLED ROUTER B

Similarly the router B has been enabled.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

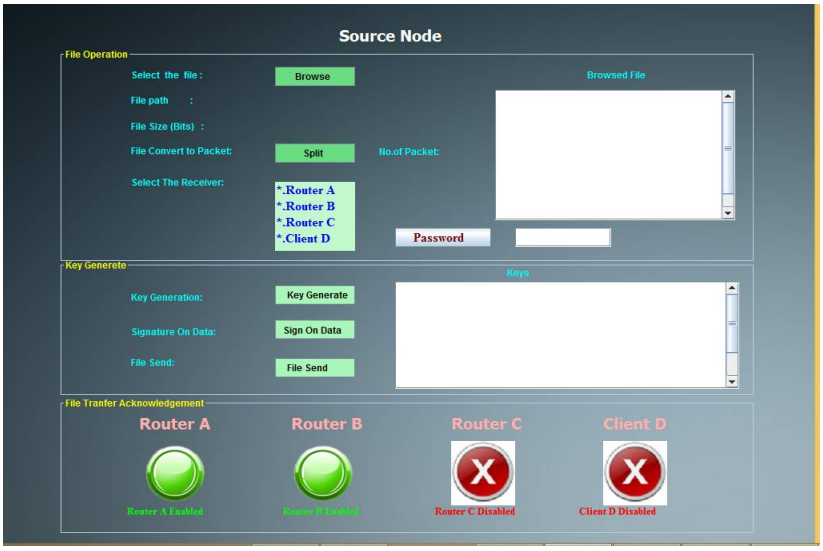

FIGURE 1.6-SPLITTING OF DATA PACKETS

Once the routers has been enabled the browsed file will be split into packets and the required routers are selected. And when this is done a particular key will be generated.

V.CONCLUSION

In this paper, we have proposed a secure handover key management scheme in the third-party owned MRN scenario, which mainly concentrates on establishing secure session keys between the on-board UEs and thetarget DeNB while exploiting the third-party owned MRNs during the key establishment without disclosing the content of the session keys.Detailed analysis shows that the proposed secure handover keymanagement scheme can successfully establish the session keys, achieve the requirements of the backward and forward key separation, and resist the collusion attack.We also conducted the performance evaluation in terms of computational cost, communication overhead, and storage cost to demonstrate theeffectiveness and efficiency of our proposed scheme, and the trade-off between the number of MRNs and the computational latency was deliberately discussed In our future work, we plan to carry on smart-phone based and real public transportation scenario based experiments to verify the effectiveness andefficiency of the proposed handover key management scheme.

REFERENCES

[1] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: a study on qos security threats and countermeasures using intrusion detection system approach," Int. J. Communication Systems, vol. 25, no. 9, pp. 1189–1212, 2012.
[2] Z. Zhou, M. Dong, K. Ota, G. Wang, and L. T. Yang, "Energy-efficient resource allocation for D2D communications underlaying cloud-ranbased LTE-A networks," IEEE Internet of Things Journal, vol. 3, no. 3, pp. 428–438, 2016.
[3] J. Wu, M. Dong, K. Ota, L. Liang, and Z. Zhou, "Securing distributed storage for social internet of things using regenerating code and blom key agreement," Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1133–1142, 2015.
[4] L. Costantino, N. Buonaccorsi, C. Cicconetti, and R. Mambrini, "Performance analysis of an LTE gateway for the iot," in 2012 IEEEInternational Symposium on a World of Wireless, Mobile and MultimediaNetworks, WoWMoM 2012, San Francisco, CA, USA, June 25-28, 2012, 2012, pp. 1–6.
[5] R. W. H. Jr., M. L. Honig, S. Nagata, S. Parkvall, and A. C. K. Soong, "Lte-advanced pro: part 1 [guest editorial]," IEEE CommunicationsMagazine, vol. 54, no. 5, pp. 74–75, 2016.
[6] Z. Zhou, M. Dong, K. Ota, and Z. Chang, "Energy-efficient contextaware matching for resource allocation in ultra-dense small cells," IEEEAccess, vol. 3, pp. 1849–1860, 2015.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

[7] M. Peng, Y. Li, Z. Zhao, and C. Wang, "System architecture and key technologies for 5g heterogeneous cloud radio access networks," IEEENetwork, vol. 29, no. 2, pp. 6–14, 2015.
[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[9]J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," FutureGeneration Comp. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
[10] "Technical specification group radio access network; mobile relay for evolved universal terrestrial radio access (e-utra)," 3GPP TR 36.836, 2012.
[11] L. Chen et al, "Mobile relay in LTE-advanced systems", *IEEECommun. Mag.*, vol. 51, no. 11, pp. 144-151, Nov. 2013.
[12] J. Kokkoniemi et al, "Performance evaluation of vehicular LTE mobile relay nodes", *Proc. 24th IEEE Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*,pp. 1972-1976, 2013.
[13] O. Altrad, S. Muhaidat, "Intra-frequency handover algorithm design in LTE networks using Doppler frequency estimation", *Proc. Workshops Glob.Commun.Conf. (GLOBECOM)*, pp. 1172-1177, 2012.
[14] Y. Sui et al., "Moving cells: A promising solution to boost performance for vehicular users", *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 62-68, Jun. 2013.
[15] N. Lin, X. Huang, X. Ma, "Analysis of the uplink capacity in the high-speed train wireless communication with full-duplex mobile relay", *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, pp. 1-5, 2016.
[16] F. Y.-S. Lin, C.-H.Hsiao, K.-C.Chu, Y.-H.Liu, "Minimum-cost QoS-constrained deployment and routing policies for wireless relay networks", *J. Appl. Math.*, vol. 2013, pp. 1-19, 2013.
[17] C. Lai, H. Li, R. Lu, R. Jiang, X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks", *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 1011-1016, 2014.
[18] G. M. Køien, "Mutual entity authentication for LTE", *Proc. 7th Int. Wireless Commun. Mobile Comput.Conf. (IWCMC)*, pp. 689-694, 2011.
[19] D. Forsberg, "LTE key management analysis with session keys context", *Comput. Commun.*, vol. 33, no. 16, pp. 1907-1915, 2010.
[20] "Technical specification group service and system aspects; 3GPP system architecture evolution (SAE)", Sep. 2012, [online] Available: http://www.3gpp.org/.

.