SECURE AND SMART MEDIA SHARING BASED ON DIRECT COMMUNICATIONS AMONG MOBILE DEVICES UNDERLYING IN LTE-A CELLULAR NETWORK

Sambasivam Ramasubramanian, Sam Chung, Ling Ding
Computer Science and Systems
Institute of Technology
University of Washington
Tacoma, USA
{samba84, chungsa, lingding}@uw.edu

Seungwan Ryu
Chung-Ang University
Anseong, Korea
ryu@cau.ac.kr

Abstract* – Cellular network service providers are trying to expand their capacity to accommodate the increasing mobile traffic demand by adopting new mobile technologies like user proximity based Device-to-Device (D2D) communication underlying existing Long Term Evolution-Advanced (LTE-A) cellular network, which is a promising technology to overcome legacy cellular network's congestion. D2D communication is a new paradigm to enhance legacy LTE-A cellular network performance. However, there are several challenges to be overcome: 1) what will be the trending technology for overcoming cellular network data traffic congestion? 2) How can we overcome security threats and high pricing for data services? And 3) how can users earn revenue by media sharing? To date, there are many papers available on D2D communications in cellular networks. But, there is no paper on proposing security measures and business models for D2D communications in cellular networks. We propose a secure and smart solution that answers the three challenges thereby enhancing efficiency of D2D communications in a smart and secure manner. Our solution will demonstrate that the proposed application level security framework will output reduced network congestion, better pricing schemes, auctioning system and less or no security threats than the current legacy non-D2D communication models.

Keywords: *D2D Communication, Long Term Evolution-Advanced (LTE-A), Security Framework.*

I. INTRODUCTION

Mobile wireless communication has seen numerous advancements right from its discovery. The sales of smartphones and tablets are booming in today's scenario due to its enormous enhancements in mobile device services and applications. Cellular subscribers download applications, games, music, and videos from various online stores via their cellular network. The number of cellular subscribers increases drastically day-by-day as a cellular network operator tries offering the best services due to the immense competitive market. This makes the cellular operator to consider requirements of users in various perspectives. Cellular subscribers pay network operator for data traffic and app store for content download.

The widespread of smartphone applications of various platforms, availability of all application development platforms, and distribution marketplaces are encouraging innovation in applications on a very high scale leading to the extensive growth of number of applications, the usage of the applications, and the usage of mobile data networks [2].

In recent days, D2D communication has gained increasing popularity among cellular network operator even though this new technique is waiting for commercialization. D2D communication enables two or more mobile devices in proximity of each other to establish direct local links with any physical medium of their choice, within an ad hoc network without the support of cellular network or with assistance from cellular network to perform direct data transfer. The merits of

D2D communication include proximity communication, traffic offload from cellular networks, and reduced service cost.

In order to transfer media based on D2D communication among mobile devices underlying LTE-A cellular network, we challenge three problems: 1) how can we reduce the amount of traffic flow in radio link between UE, and eNodeB? 2) How can we reduce high data traffic price by using D2D? And 3) how can we reduce vulnerabilities of D2D?

For the best outcome of D2D communication, there are three vital aspects (Fig. 1), which should be considered concurrently.

1. Technology: D2D communications can take place with any existing Mobile device Peer to Peer (P2P) technology. For Example Bluetooth, WiFi Direct, LTE-A Direct, etc.
2. Business Model: D2D communications should hold service pricing schemes, pricing policies, and revenue flows between Network Element's (NE) for various use case scenarios.
3. Security: UE's free from all possible vulnerabilities like spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege which pose a major privacy, and security threats if not been handled.

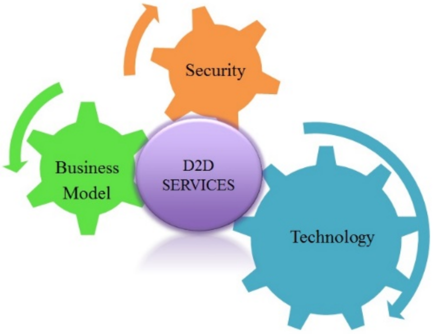


Fig. 1. Three Vital Items of D2D Communication

Assuming that Technology for D2D communication has been identified and implemented, there are still many issues, which need to be addressed before the concept of D2D communication can be implemented and commercialized. These major challenges include identifying and implementing an application level security framework for UE's which is the major focus of this paper.

This paper is organized as follows: Section II discusses about the evolution of various wireless communication technologies, smartphone effects and challenges of D2D communication. Section III briefs the three types of D2D services namely Ad-Hoc type, Agent type and Mesh type. Section IV introduces the legacy LTE-A and D2D communication architecture along with comparison of Legacy LTE-A and D2D communication security threats. Also it discusses about the evolution of PC security to Mobile security is briefly discussed which gives basic security framework for D2D communication. Section V discusses two efficient security procedures which satisfies three items: 1) network congestion alleviated by designing systematic D2D model architecture, 2) high pricing reduced by proposing acceptable and efficient procedures which provides cost effective pricing schemes, and 3) vulnerabilities (security threats) reduced by designing reliable Security mechanism which overcomes all sorts of security threats.

II. Research Background

A. *Evolution of Wireless Communication Technologies*

Wireless Mobile communications systems have revolutionized the way people communicate, joining communications, and mobility. History of wireless has achieved a long way in a remarkably short time. Evolution of wireless access technologies has commercially reached its fourth generation (4G/4.5G) to a speed of 1Gbps. The history of wireless access technologies has taken different paths aimed at various targets like service performance, and efficiency in an extensive mobile environment [5].

B. *Smartphones and its effects*

As per Cisco VNI & AT Kearney Analysis, Mobile Wireless communication technology is advancing too fast (Fig. 2), to deliver richer content and applications to connected mobile devices. The number of subscriptions for each Cellular network Provider also continues to grow drastically with such adverse increase in mobile data traffic.

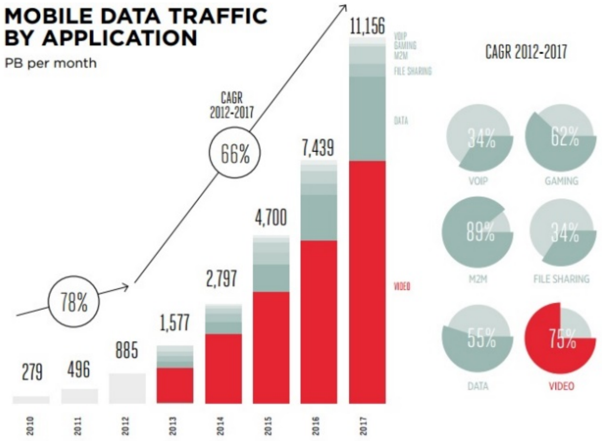


Fig. 2. Mobile Data Traffic by Application
(Source: Cisco VNI, 2013, A.T. Kearney Analysis)

Thereby, it creates a significant network capacity shortage concerns for mobile network service operators. Cellular network Providers are trying to increase the capacity in a number of ways to cope up with network congestion problems. It includes installation of more base stations (eNB), reallocation of existing spectrum with additional spectrum resources. However, these efforts are not an efficient solution but it is for a short-term backup plan [8].

C. *Introduction to D2D*

In D2D communication, UE finds its neighbor by utilizing proximity search method thereby transferring data between two or more UE's directly with less intervention of underlying LTE-A cellular network. Proximity-based D2D applications and services represent a recent advancement following the social-technological trend. The main principle of the D2D applications is to find existence of the applications running in nearby devices that are within proximity circle of each other. Adding to this technique, 3GPP has opened the opportunity to enable platform of individual choice in running proximity-based communication between devices, thereby promoting a huge opening for future proximity-based applications.

Two important services of ProSe are proximity discovery, and proximity communication. Proximity discovery is technique with which users can discovery each other's in proximity. Proximity communication is direct communication with which users can communicate with each other in proximity.

There is no boundary between proximity discovery, and proximity direct communication. Proximity discovery can act as a standalone service to users, and it doesn't always trigger proximity based direct communication. UE's can initiate D2D communication directly without proximity discovery. However UE's can use D2D communication efficiently if they know the proximity information beforehand [6].

III. CLASSIFICATION OF D2D SERVICES

A. Types of D2D

D2D communications is broadly classified into two types - D2D Network assisted and D2D Autonomous, which are shown in Fig. 3.

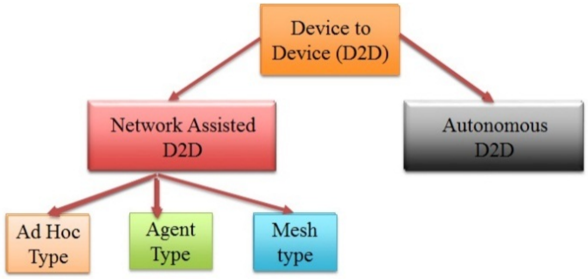


Fig. 3. Types of D2D

1. D2D Network assisted

The network plays a vital role in D2D communication. For instance, the network provides location information of devices that are located within a proximity area to assist in formation of the D2D cluster. The network is also responsible for radio link pairing between devices, and it provides radio resource management related information for D2D communications such as available spectrum band, available frame resource assignment, transmission and reception scheduling information and others. In turn, D2D Network assisted is sub-classified into three different types, namely: 1) Ad hoc type, 2) Agent type, and 3) Mesh type. The communication details of the three types will be introduced respectively as follows, using angry bird as an example.

i) Ad-hoc type (Fig. 4)

- UE1 already owns the copy of the Angry Bird game, and advertises for selling it.
- UE2 requests UE1 for the Angry Bird Game
- UE1 transfers the requested content to UE2.
- UE2 is free from data traffic cost but pays App store for the license copy of the content.

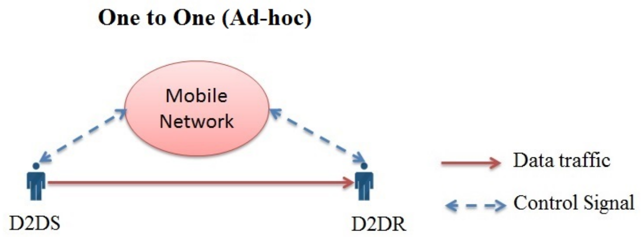


Fig. 4. Ad-Hoc D2D Type

ii) Agent type (Fig. 5)

- When several devices requests for a same content they form a cluster, and nominates one UE as an Agent (Cluster head-CH)
- The Agent UE downloads multiple copies of the content from Cellular Network as agent of all the UE's in that cluster.
- Agent UE downloads N copies from App store through cellular network, as per the cluster quantity, and then distributes the content plus license file to each UE. Therefore data traffic usage is fairly reduced.

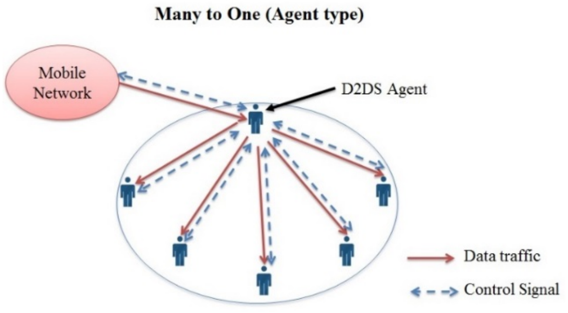


Fig. 5. Agent D2D type

- Other UE's pays Agent UE for content download, and shares data traffic cost between each other's.

iii) Mesh type (Fig. 6)

- All UE's form a cluster, and request for Angry bird game
- Mobile Network distributes the angry bird game to N users by sending 1/N part of content to each User.
- Each UE then shares its 1/Nth part of data with other UE's
- After receiving all the parts of content, UE's combine it into one file, and then install the game.
- Here the data traffic cost is reduced as instead of downloading the entire content UE's just download part of it
- Each UE pay the App store for the license copy to install the game.

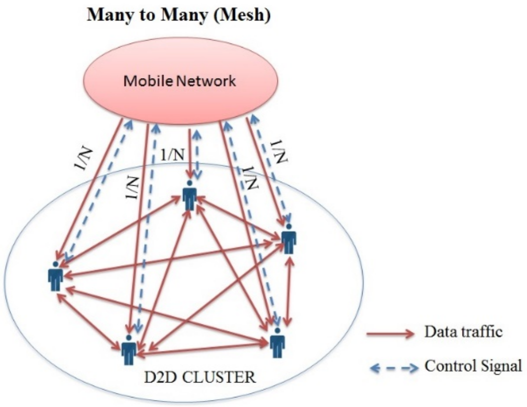


Fig. 6. Mesh D2D Type

2. D2D Autonomous (No Network assistance)

The network plays a minimum level role in the D2D communication. For Instance, the network provides only mutual authentication information when the devices are forming a D2D cluster. Then, devices use the available radio resources for D2D communication autonomously [8].

Here in this paper we only consider D2D Network assisted types in developing two Business models.

B. Legacy LTE-A wireless communication vs. D2D Communication

D2D communications underlying a LTE-A cellular infrastructure is a new technique which takes advantage of the physical proximity of mobile communicating devices, thereby increasing resource utilization, and improving cellular coverage. Like traditional cellular network systems, there exists a need to design new peer to peer communication using proximity discovery methods that increases the potential advantages of D2D communications. [1]

The main aim of D2D communication is to improvise wireless cellular system capacity by offloading cellular traffic in legacy cellular system, and without increasing the infrastructure cost. In legacy cellular system, UE's communicate via radio area uplink, core network uplink, core network downlink, and radio area downlink despite the proximity to each other. However UE's enabled with D2D technology, can communicate directly using the D2D link. D2D communications can handle data traffic without utilizing the core network load, and the additional radio network load which exists in the legacy cellular system [4].

IV. D2D THREAT TYPES AND SECURITY FRAMEWORK

A. Legacy LTE-A System

Fig. 7 gives a brief understanding of how the data traffic is handled in legacy LTE-A cellular network. Here the UE's requests for downloading an application from AppStore through its cellular network. The cellular network in turn sends the information regarding UE's to Security server for verification. Once the security server verifies the UE's, then Cellular network connects the UE's to the AppStore.

Now the UE's pay for the content to the AppStore, and AppStore in turn sends the requested data to UE's via cellular network, and informs the Content provider regarding the number of downloads for respective application. Now cellular Network charges the UE's for accessing packet data. There are much of control flow signals (marked in blue) back and forth between all components, and data traffic among AppStore, Cellular network, and UE1.

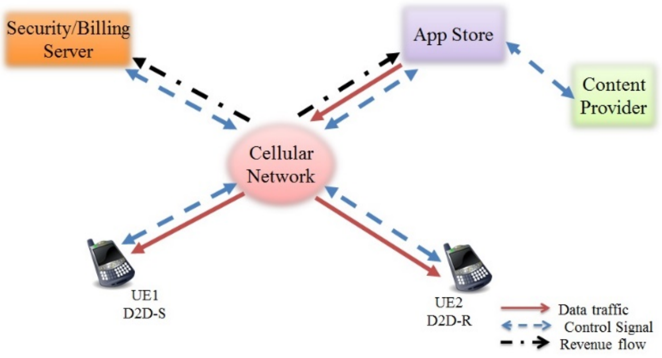


Fig. 7. Legacy LTE-A Network Architecture

B. D2D Communication Architecture

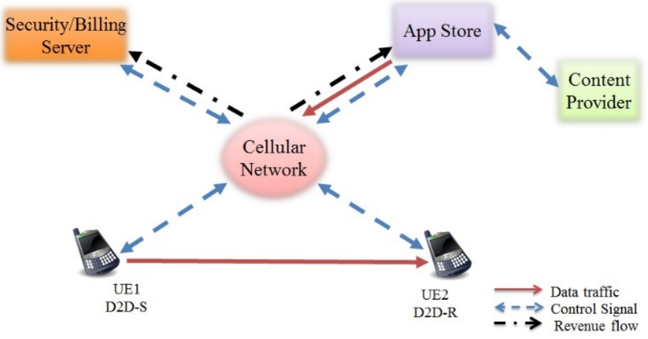


Fig. 8. D2D Communication Architecture

The general architecture of D2D communication (Fig. 8) is such that UE1 shares the content to UE2 by verifying the UE2 with the LTE-A cellular network. Therefore, the UE2 is free from paying huge data traffic cost, and just end up in paying meager amount to the UE1 for usage of D2D communication service by which cellular network operator is free from heavy network congestion due to rise of individual data downloads from each mobile subscribers.

C. D2D security issues

Currently we have identified that there are three possibilities of Security threats in D2D communication.

1) As seen in Fig. 9, Fake D2D-S (advertisers) post advertisements which could lead legitimate recipients facing

high risk by sharing their user information when requesting for the content download.

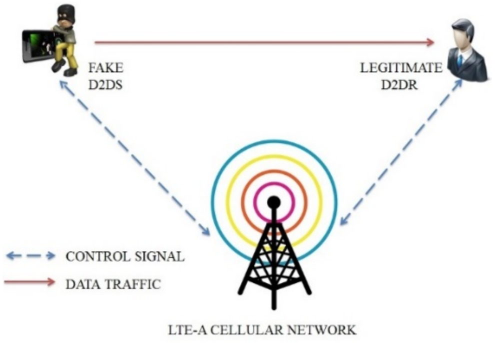


Fig. 9. D2D Threat Type-1

2) As seen in Fig. 10, Fake D2D-R (recipients) send bulk download requests to legitimate advertisers, thereby loading their device with numerous fake requests along with other vulnerable threats.

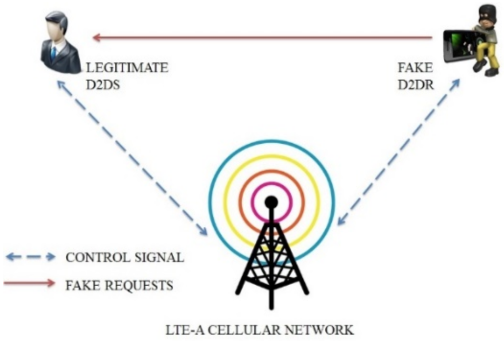


Fig. 10. D2D Threat Type-2

3) Legitimate advertisers, and recipients been attacked by the Man-in-the-Middle (MITM) who in turn eavesdrop the secured information or the content, and thereby gain by cracking the same. (Fig. 11).

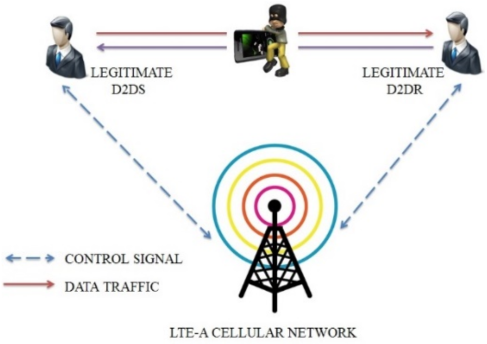


Fig. 11. D2D Threat Type-3

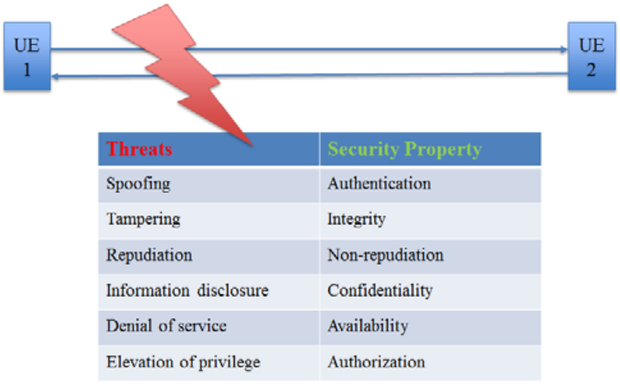
Throughout the world, enormous smartphone growth and the emerging mobile ecosystem has led to key concern of mobile application privacy for users. This issue is still waiting for the whole of the mobile ecosystem to address it making the users feel comfortable in using mobile applications. The key concerns includes collection of user information, device IDs, user's behavior, location data, access to contact lists, and other user generated data without the knowledge or consent of mobile users [7].

Table 1. Network Elements vs. Security Threats [3]

Elements	S	T	R	I	D	E
Data Flows		Y		Y	Y	
Data Stores		Y		Y	Y	
Processes	Y	Y	Y	Y	Y	Y
Interactors	Y		Y			

S – Spoofing, T – Tampering, R – Repudiation, I - Information Disclosure, D - Denial of Service, E - Elevation of privilege, Y – Yes

Thereby for each type of UE threats, a security property is identified (Fig. 12) using "STRIDE approach". List of various threats and each of its security properties is shown in Fig. 12. Based on the "STRIDE approach of Microsoft" [3] which has been applied for Computer network security (Table 1), various types of Application level security for D2D communication have been studied, identified and matched PC security.



Threats	Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Fig. 12. Various UE Threats

As per Table-1 the following components in D2D architecture has been identified.

- *Data Flows*: Control Signal flow, Data traffic flow, Revenue signal flow
- *Data Stores*: Authorization, Authentication & Accounting (AAA) Server Database, App Store Database
- *Processes*: UE Advertising, UE Download request, D2D data transfer between UE's, User authentication
- *Interactors*: Mobile Network, UE, Security/Billing Server, App Store, Content Provider.

V. D2DCOMM OVERALL FRAMEWORK

In this capstone project, we have built a prototype for demonstration purpose by designing two web servers namely Appstore server and Operator Server using Java, Spring MVC, RESTful Web services, JSON, JSP. Also we have built one Android Application package file (APK) namely D2DFileTransfer App. This D2DFileTransferApp works for mobiles only with Wireless Fidelity Direct (WiFi-D) functionality which is a trending P2P technology. These are the three major components used for demonstration along with PostgreSQL Database.

Assuming UE1 (i.e. D2D-S) who already holds the APK content, advertises for the same using D2DFileTransferApp. The UE2 (i.e. D2D-R) which also holds the D2DFileTransfer App and being in the proximity discovery radius of D2D-S gets pairing request from D2D-S. Once the D2D-R accepts the request, D2D-S starts sending the APK file along with user device info like Sender International Mobile Equipment Identity (IMEI), File Name to D2D-R. Once it receives the file the D2D-R forwards the related information received from D2D-R along with the calculated Hash value for APK file using MD5 algorithm to Operator Billing DB server. The Operator Billing Server forwards the received hash value to Appstore Billing server to verify the file correctness. If the APK file name and APK file hash value matches with AppStore Server DB then Operator Billing server receives a positive response through REST/JSON services. Else it gets a negative response about the file availability in the Appstore DB. Based on the response from Appstore server, the Operator Billing server sends a safe/unsafe message to D2D-R using REST/JSON services and also performs billing for both D2D-S and D2D-R. The above process takes place between 1 second to ‘N’ minutes depending upon the file size being transferred between two mobiles. In this case D2D-R pays Operator Billing for App cost and usage of D2D services, thus piracy or illegal copy of contents is highly prohibited in this business model. Also D2D-S earns revenue by bidding through a truthful auctioning system.

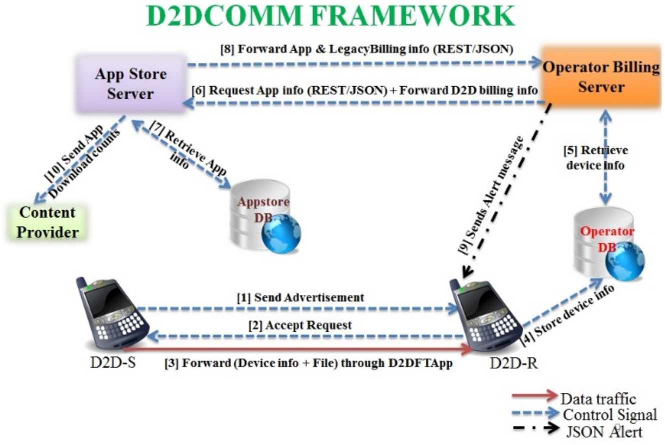
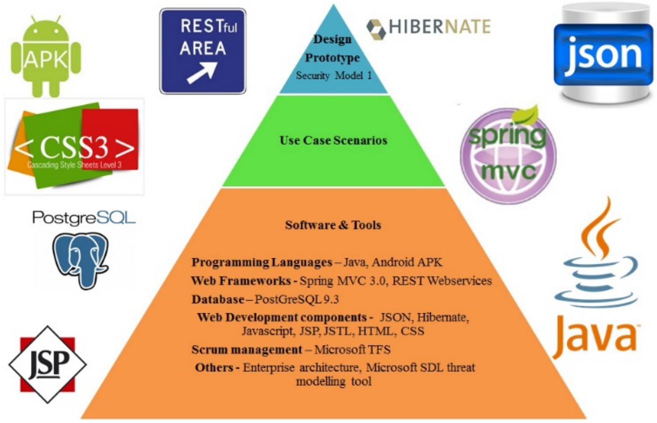


Fig. 13. Proposed D2D Business Model 1

The above framework clearly shows that

1. Network Congestion gets alleviated
2. High user pricing (service price + content price) gets reduced.
3. Possibilities of various UE vulnerabilities (security threats) get reduced to maximum extent.

The above framework for this project was achieved using the below tools.


APK
RESTful AREA
Design
Prototype
Security Model 1
HIBERNATE
json
< CSS3 >
Cascading Style Sheets Level 3
Use Case Scenarios
spring mvc
PostgreSQL
Software & Tools
Programming Languages – Java, Android APK
Web Frameworks - Spring MVC 3.0, REST Webservices
Database – PostGreSQL 9.3
Web Development components - JSON, Hibernate, Javascript, JSP, JSTL, HTML, CSS
Scrum management – Microsoft TFS
Others - Enterprise architecture, Microsoft SDL threat modelling tool
JSP
Java

VI. CONCLUSION AND RELATED REMARKS

In this project, we first introduce the 3GPP LTE-A and D2D architecture. By identifying various D2D security threats, we then designed a basic security framework for UE D2D communication followed by a detailed security procedure. In this security procedure, the legacy LTE-A cellular network's bandwidth is least used for packet data traffic and mostly used for control signal flow. Thus the proposed D2D communication security framework and procedures improves the trust and cost wise benefits for the cellular users and network bandwidth oriented benefits for the cellular operators.

REFERENCES

[1] Gábor Fodor, Erik Dahlman, Gunnar Mildh, Stefan Parkvall, Norbert Reider, György Miklós, and Zoltán Turányi “*Design Aspects of Network Assisted Device-to-Device Communications*.” Ericsson Research.

[2] 4G Americas White Paper “*New Wireless Broadband Applications and Devices*.” May 2012.

[3] *Uncover Security Design Flaws Using The STRIDE Approach*, Accessed on May 13, 2013.

[4] Mi Jeong Yang, Soon Yong Lim, Hyeong Jun Park, and Nam Hoon Park - IEEE VT Magazine 2013, “*Solving the Data Overload - Device-to-Device Bearer Control Architecture for Cellular Data Offloading*”,

[5] Amit Kumar,Dr. Yunfei Liu, Jyotsna Sengupta, Divya “*Evolution of Mobile Wireless Communication Networks:1G to 4G*.” IJECT Vol. 1, Issue 1, December 2010, ISSN : 2230-7109

[6] Huawei R&D team “*Future smartphone solution white paper*”, Issue 2.0, September 2012.

[7] “*The Mobile Economy 2013*.”, A.T.Kearney and GSMA, Accessed on 3 June 2013.

[8] Seungwan Ryu, Sei-Kwon Park, Nam-Hoon Park, and Sam Chung, “*Development of Device-To-Device(D2D) Communication Based New Mobile Proximity Multimedia Service Business Models*”, 1st Workshop on Management Information Systems (MIS) in Multimedia Art, Education, Entertainment, and Culture (MIS-MEDIA 2013), in conjunction with ICME 2013 IEEE International Conference on Multimedia and Expo (ICME 2013), July 15th-19th, 2013, San Jose, California, USA