Neighbor and Service Discovery Protocols with Security Enhancement for Device-to-Device Communication in LTE/LTE-A Cellular Networks

By

Anuradha Bista and Milka Radin

Supervisor: Frank Y. Li

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information and Communication Technology

Department of Information and Communication Technology

Faculty of Engineering and Science

University of Agder

May 26, 2015

Abstract

Device-to-Device (D2D) communication has become one of the most popular topic in the 5th generation (5G) mobile communication technology. D2D offers opportunities for access to services through direct neighbor device connection with or/and without base station (BS) assistance. Some of the possible improvements using D2D communication include high data rate, network offloading and range extension, as well as commercial and social proximity services networking. Although a lot of studies exist in the research community, D2D communication with one of the end users are located outside the cellular network coverage has not received enough attention. Some of the problems faced in this case are discovering process of neighbor user equipment (UE) and services, as well as designing suitable and secure protocols for D2D communication.

Toward these problems, two protocols (reactive and proactive) for neighbor and service discovery are proposed in this thesis. Implementation of reactive protocol, proactive protocol, simulation and validation are shown. Furthermore, the proposed protocols are improved with additional security enhancement. The overhead calculation results show that reactive protocol achieves better performance when data traffic load is lower whereas proactive is preferred with higher traffic load in D2D communication.

Keywords: D2D communication, ProSe discovery, protocol overhead, security enhancement and partial support.

Preface

This thesis is the result of the IKT590 Master's thesis project, which is corresponding to 30 ECTS points, at the Department of Information and Communication Technology (ICT), Faculty of Engineering and Science, University of Agder (UiA), Norway. This Master's thesis work started from January 2, 2015 and ended on May 26, 2015.

We would like to thank our supervisor Frank Y. Li for his valuable guidance and supports during this thesis. Special thanks to our families Bista and Radin for continuous support and encouragement.

Anuradha Bista and Milka Radin
Grimstad
May 26, 2015

Contents

List of Figures

List of Tables

Abbreviations

3GPP	3rd generation partnership project
4G	4th generation
5G	5th generation
AS	application server
BS	base station
CA	carrier aggregation
CIAAA	confidentiality, integrity, authentication, availability and accessibility
D2D	Device-to-Device
DoS	Denial of service
DSig	digital signature
E-UTRAN	edvolved-universal mobile telecommunications system terrestrial radio access network
eNB	evolved node base station
EPC	evolved packet core
EPS	evolved packet system
FDD	frequency division duplex

HeNBs	home evolved base stations
IMT	international mobile telecommunication
IoT	internet of things
IP	internet protocol
ITU	international telecommunication union
LTE	long term evolution
LTE-A	long term evolution-advanced
METIS	Mobile and wireless communications enablers for the twenty-twenty information society
MIM	Man in the middle
OFDMA	orthogonal frequency fivision multiplexing access
PCs	personal computers
PDF	probability density function
PLMN	public land mobile network
PROMELA	process meta language
ProSe	proximity services
PubK	public key
QoS	Quality of Service
SC-OFDMA	spatial carrier sense orthogonal frequency division multiple access
SDL	Specification and description language
SNR	signal to noise ratio
SPIN	Simple promela interpreter
TDD	time division duplex

UE	user equipment
UE-E	UE-End
UE-R	UE-Relay
UV	ultraviolet
XOR	exclusive OR

Chapter 1

Introduction

D2D is becoming a hot topic in wireless communication and mainly investigated under the perspective of providing new commercial services or public safety proximity services (ProSe) [1]. This chapter gives an overview of D2D communication which is one of the promising technologies for the 5G mobile communication system. It provides the background of neighbor and service discovery protocol as well as a general analysis of D2D security. Problem statement, problem solution, methodology and thesis outline are presented herein.

1.1 Background and Motivation

Due to the rapid growth of applications data of smartphone, tablet and personal computers (PCs), the amount of cellular traffic is increasing day by day. Therefore, it becomes difficult to the network infrastructure to response to all requests in a timely manner. There are many factors which make the network infrastructure unable to serve users. For instance, traffic overload/congestion in network, power outage in system, natural disaster, and terrorist attack [2]. In case of natural disaster and terrorist attack, it is necessary to notify the users (for example family and friends) about their condition. In such scenarios, it becomes impossible for people to reach to one another or/and help center with destroyed cellular network. Hence, D2D is adopted by the 3rd generation partnership project (3GPP) in long term evolution-advanced (LTE-A) (Release 12) [2] in order to overcome

from previously specified problems. Beside public safety scenario, D2D also has commercial usages. For example, if any restaurant wants to advertise its food discount scheme to its nearby mobile user then it can broadcast the messages either via BS or via ProSe enabled UE. Any interested UE which is in the proximity distance to restaurant's UEs can reserve the table or/and food directly using its ProSe without passing through the BS.

The UEs, which are sending and receiving data traffic, must be assured that their data is not accessible to the other UEs and UEs are not compromised. Therefore, security plays an important role to successfully conduct the D2D communication in cellular networks. Generally, in regular LTE-A cellular networks, the BS and UEs adopt the standard LTE-A security mechanism. Operators have responsibility for securing the network by using strong and reliable methods of authentication, authorization and integrity [3]. During D2D communication process, infrastructure like BS does not assist to establish the secure connection between UEs [4]. Due to security weaknesses in D2D protocols, attackers can steal the personal information from core network, modify user's information and invade user's privacy by breaking the user's devices or network [3]. A protocol is said to be secure if it satisfies the minimum-security requirements such as confidentiality, integrity, authentication, availability and accessibility (CIAAA) [5]. Various encryption/decryption algorithm should be used to secure the information exchanged among UEs.

Adding D2D communication in cellular system maintains the quality of existing voice communication because it will decrease traffic via BS [6]. UEs inside the network coverage area can also get benefits from D2D communication such as higher data rates due to better channel quality and less power consumption [6]. Bluetooth and ultraviolet (UV) are few unlicensed technologies used for communication among UEs. High interference, higher energy consumption and low area coverage are one of the problems that Bluetooth and UV are facing. D2D communication is an option to overcome from such problems. It potentially saves energy consumption by reusing cellular resources, reducing interference, utilizing peer-to-peer links for users in proximity of each other [7], as well as it is licensed technologies.

Even though D2D has promising features, there are still many task in order to im-

plement such a new communication where end users are located inside and outside coverage area. Device discovery, resource allocation and security are some of the key challenges D2D communications are facing in above mentioned scenario. In order to implement D2D communication, UE should discover the nearby UEs in its proximity area. While applying device discovery procedure, it must fulfill the general requirements like fast discovery, low energy consumption and minimize interference [8]. Since the devices are mobile, change in location of the device is expected. Therefore, discovering of nearby devices become difficult. The availability of resources for D2D communications is one of the challenging factors due to limited resources for D2D communication. For this reason, it is vital to adopt the communication protocols that utilize less resources.
Furthermore, security aspects of D2D communication has not been addressed enough for the scenario where one of the end users is not covered by BS. Two UEs participating in D2D communication must ensure that they are communicating with legitimate UEs and the information they are receiving are correct. If security mechanism is not applied during device discovery or communication process, the information might be altered or misused by a malicious user. Therefore, it becomes necessary to secure the data during UEs discovering and/or communication process. Preserving user's information and keeping it secret while communicating is another challenging factor. This is very critical and sensitive situation, which must be addressed before implementing D2D communication in the cellular networks. There are many research work are performed either in the security of D2D communication or in neighbor and service discovery protocol design, but only limited studies have been performed which combined neighbor and service discovery protocol design with its security enhancement. This motivate us to investigate on security enhancement of D2D communication protocol.

1.2 Problem Statement

Increased network spectral efficiency, energy efficiency, reduced transmission delay, offload traffic for BS and less congestion in the cellular core network are few advantages of D2D communication [9]. Despite of having aforementioned advantages, D2D introduces some complications. For D2D pair, discovering ProSe

UEs as well as ProSe services within proximity distance is one of these challenges. Due to the limited resources capacity for D2D communication, adopting communication protocol which utilizes less resource is itself one challenging factor for D2D communication. Security in such communication is important because there is no any central equipment to control the security mechanism between UEs. An intruder may attacks the link between UEs or break down the UEs to steal the valuable information. Therefore, it is necessary to address the neighbor and service discovery protocol with security enhancement mechanism. Two scenarios are identified and one of them is selected for protocol design.

Scenario: one of the UE is outside of the cellular coverage area. More explanation about selected scenario can be found in Sec.3.2. Below are a few fundamental questions which need to be addressed before commercial deployments of D2D communications for given scenario:

- How neighbor UEs and services are discovered when one of the UEs is outside cellular coverage area?
- How to design and select a suitable protocol for the above mentioned scenario?
- How to secure the handshake process between UEs in the designed protocol?

1.3 Problem Solution

The proposed protocol design is based on a hybrid network design, cellular and ad-hoc networks. UE-Relay (UE-R)[1] user is the main communication device in the connection and it should support two different radio spectrum. One for wireless as ad hoc network and another for mobile networks as part of cellular backbone. In both connections, the handshake procedure should be done for neighbor and service discovery before UEs actually start to communicate with each other. UE-R or UE-End (UE-E)[2] could initiate the neighbor and service discovery process. Two protocols were proposed in this thesis, proactive and reactive protocols.

[1] UE-R is a UE which is inside network coverage area.
[2] UE-E is a UE which is outside network coverage area.

UE-R initiates discovery process using proactive protocol whereas UE-E initiates discovery process using reactive protocol. Firstly, our protocols focus on one UE-E user and one UE-R user, but the protocols are equally applicable for many UE-E users and one UE-R user. However, the number of UE-E users should be limited according to the capacity of UE-R. In both protocols, BS does not have any role to discover the UE-E(s). We have considered three different cases of occurrence of D2D request to compare the performance of both protocols. Numerical analysis of protocol overhead was performed in MATLAB simulation environment and compare the results accordingly.
Security in cellular network is becoming more and more important as user shares their personal sensitive information through the cellular devices. Hence, it is necessary to detect any malicious behavior before devices start to exchange messages. In the proposed protocols, UEs will authenticate each other within the handshaking process so that the UEs can be assured that they are communicating with legitimate UE. Upon authentication protocol, they agree on common secret key which will be used for encryption/decryption of messages. Diffi-Hellman key exchange algorithm was used to establish a common secret key between UEs.

1.4 Objectives

A secure and reliable D2D commutation must enable UEs to communicate with each other without the support from BS in a scalable, efficient, and secure manner. The objectives of this study are as follows:

- To gain a deep understanding of D2D commutation, how D2D communication works and how neighbor and service discovery protocols work.
- To investigate on different use cases/scenarios suggested by 3GPP for device discovery process and analyze the existing D2D communication protocols.
- To purpose two handshake protocols in the envisaged scenario.
- To purpose the security enhancement protocol based on Diffi-Hellman key exchange algorithm.

- To implement and validate the proposed protocols and security enhancement protocol .
- To evaluate the performance of the proposed protocols and compare them in terms of protocol overhead.

1.5 Thesis Outline

The remainder of this Master's thesis is organized as follows:

- Chap. 2 discusses about enabling technologies as a part of D2D communication that 3GPP organization made.
- Chap. 3 describes our proactive and reactive protocols design with given scenarios without security mechanisms.
- Chap. 4 presents the implementation of proposed protocols as well as validation based on protocol overhead.
- Chap. 5 discusses security challenges and threats of D2D communication as well as six ways handshake protocol for authentication and establishment of secret key.
- Chap. 6 represents conclusions and future work.

Chapter 2

Related Work and Enabling Technologies

Nowadays, there are many ongoing studies in the area of D2D communication including device and service discovery and D2D security. In this chapter, the general concepts related to D2D communication as well as what other researcher already have done in this field are presented.

2.1 Concepts and Enabling Technologies

2.1.1 Proximity based services (ProSe)

ProSe are services that can be provided by the 3GPP system based on UEs being in proximity to each other [10]. Proximity means the link between UEs which is favorable for D2D communication. It does not mean only the distance between them. It means the better signal quality, low signal to noise ratio (SNR), availability of resources, delay, throughput, path gain and tolerable interference [11]. If all of the above-mentioned requirements are satisfied, then only two UEs are said to be in proximity to each other. D2D communication takes place between two ProSe enabled UEs, which are in proximity with each other. The ProSe enabled UEs means an UE that support ProSe discovery and/or ProSe communication [12] ProSe enabled public safety UEs also support ProSe discovery and/or ProSe communication, but specific to public safety scenarios.

2.1.2 ProSe discovery and ProSe communication

Before enabling D2D communication, it is important to discover the nearby ProSe enabled UEs. This process is called ProSe neighbor discovery as shown in Fig. 2.1. There are two types of ProSe neighbor discovery process: direct ProSe discovery and network assisted ProSe discovery [10]. Direct ProSe discovery process enables UE to discover its neighbor without taking any help from BS. This kind of discovery occurs in public safety scenarios where network coverage is not available. In network assisted ProSe device discovery process, BS gathers all the related information to enable D2D communication. If two UEs are in proximity to each other, then BS will forward the required information to both UEs. If both of UEs are willing to start the D2D communication, then the request send by BS will be accepted otherwise rejected. This type of discovery process is mostly applicable in the case of heavy traffic overload in BS and traffic congestion in channel. Generally, there are two cases for device discovery procedure, open and restricted ProSe discovery [10]. In case of open ProSe discovery, UEs does not need permission for being discovered whereas in restricted ProSe discovery case, permission is required from the UE for being discovered.

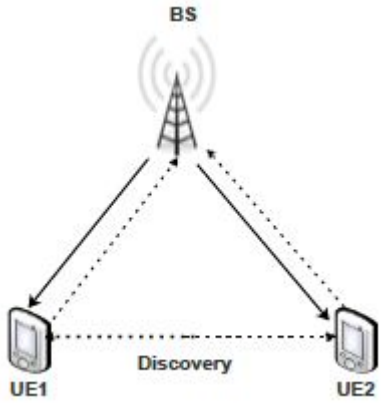


Figure 2.1: Neighbor and service discovery.

According to [1] there are two models for direct discovery, model A and model B. In case of model A, UE broadcasts its identity to start D2D communication

as shown in Fig. 2.2. If UE1 wants to start D2D communication then it will broadcast the message *"I am here"* then if any other UEs in the proximity area are interested will respond to the message. In model B, UEs either already know

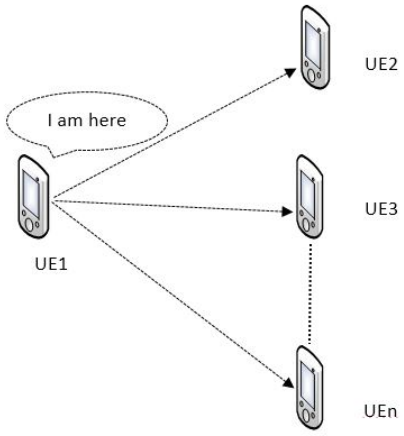
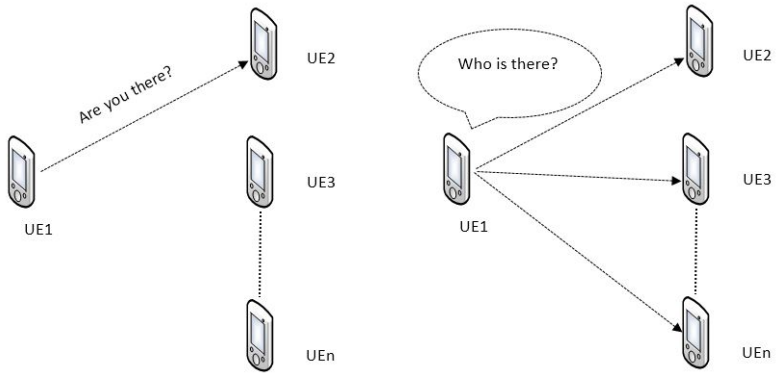


Figure 2.2: Model A direct discovery.

the identity of another UEs with whom it wants to start D2D communication as shown in Fig. 2.3a or ask if anybody is there as shown in Fig. 2.3b. In the



(a) (b)

Figure 2.3: Model B direct discovery (a) Are you there? and (b) Who is there?

discovery process, two UEs have different responsibilities namely announcing and monitoring. UE who sends the discovery request is called announcing UE and UE who processes the request is called monitoring UE. Announcing UE announces

certain information, which might be useful for other UEs that are proximity to announcing UE. Monitoring UE monitors the received information and process it. After UEs discover each other, two UEs can make a direct link between them, but it is not necessary that UEs must participate in D2D communication. In this condition their conversations are called ProSe communication [13]. Before UEs start to communicate with each other, UEs should be registered and authorized to use the ProSe services and communication in ProSe application server (AS). Once devices discover each other, they start to communicate with each other as shown in Fig. 2.4.

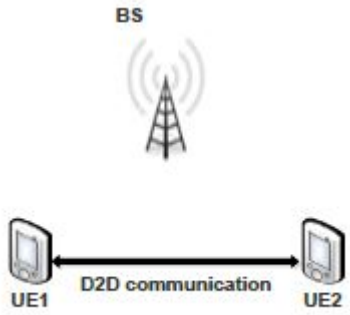


Figure 2.4: Fundamental D2D communication.

According to [1] there are two different modes for ProSe direct communication. The first mode of communication is network independent direct communication. In this mode, direct communication does not need network assistance to authorize the connection. The communication in this case is performed by using the locally available information from the UEs. This type of communication is applicable in ProSe direct one-to-one communication, ProSe direct one-to-many communication and pre-authorized ProSe enabled public safety UEs regardless of whether UEs are served by edvolved-universal mobile telecommunications system terrestrial radio access network (E-UTRAN) or not. The second mode of communication is network authorized direct communication. In this case, UEs require network assistance by evolved packet core (EPC) to authorize the connection. This

mode of communication is applicable in ProSe direct one-to-one communication, when both of the UEs are served by same E-UTRAN.

2.1.3 ProSe application server

In the cellular network, BS exchanges data traffic with a large number of UEs. During the process of establishing D2D communication, UE should deliver information about its ID as a source address, destination ID as a unique address of proximity UE, type of D2D service that is required and location to BS. All these data are saved in a database device called ProSe AS. Moreover, the main function of AS is to provide authenticity and authorization of UEs. Sometimes, AS may be installed into BS as one operation equipment. Also, AS may represent a separate device that is connected with BS as a part of a cellular network.

2.1.4 Unicast, multicast and broadcast

There are three different ways of communication in D2D, unicasting, multicasting and/or broadcasting [2]. Unicast communication means transmitting ProSe related information to one particular UE. In this case, announcing UE already knows the identity of monitoring UE. For example, UE1 wants to download some application and already knows that UE2 has such type of application. Therefore, UE1 sends discovery request directly to UE2 and after accepting UE1 request by UE2, UE1 could download the application from UE2. If ProSe communication occurs between one-to-many UEs in proximity, then such type of communication is called multicasting ProSe communication. Information is transmitted to a certain number of UEs. For example, in case of some natural disaster scenario the rescue team can communicate using one-to-many ProSe communication. One leader can give instruction to other team members about the direction and task.
In broadcast communication, either BS or UE broadcast the discovery messages within the proximity. BS broadcasts the information about the ProSe enabled UEs and ProSe services. UEs broadcasts its own information and willingness to participate in D2D communication and other related information. It is one-to-all type of ProSe communication among UEs. For example, if one Pizza restaurant in the city wants to advertise its discount scheme to the customer nearby the restaurant.

The restaurant (UE) broadcasts the advertise message, so all the ProSe enabled UEs in proximity to restaurant's UE can get the messages.

2.1.5 Reactive and proactive protocols

Reactive and proactive are two protocols for neighbor and service discovery. Both protocols have their own advantages and disadvantages. In proactive protocol, BS will notify availability of ProSe services to the UE by sending multicast messages periodically. If UE has D2D traffic to send, then it replies to the advertisement telling the BS about its ProSe discovery request. It is possible to serve D2D UEs by different BS. In reactive protocol, UE initiates the service discovery protocol whenever it needs to establish D2D communication with other UEs in the network. The main difference between these two protocols represents a UE that will initiate D2D communication. By using reactive protocol, UE always starts D2D connection with neighbor and service discovery process. That means UE will send D2D request message when it needs specific information from proximity UEs. On the other hand, BS is responsible for broadcasting service advertisement messages if proactive protocol is used. Proactive protocol is *"always on"* mechanism whereas reactive protocol is *"on demand"* mechanism.

2.2 Tools for Protocol Design, Implementation and Validation

The following tools are used for protocol design, implementation and validation:

- Simple promela interpreter (SPIN) model checker [14] is used as a formal protocol verification tool to verify the proactive and reactive protocol in D2D communication. SPIN is a verification tool which simulates a model either randomly, interactively or/and guided [15]. It exhaustively checks process meta language (PROMELA) model against correctness properties. Mainly, SPIN is used to verify the multi threaded software programming. It is not used to verify any hardware circuit. It has wide area of application such as data communication protocols, operating system, switching sys-

tems, concurrent algorithms, railway signaling protocols, control software for spacecraft and nuclear plant [15]. Among others.

- Specification and description language (SDL) [16] (Edraw Max7 tool) diagram is used to graphically represents our protocol design from the point of view of BS, UE-E, UE-R and AS. SDL provides the graphical and textual representation. SDL diagram is normally used to model the state machines in the telecommunications, aviation, automotive and medical industries which can be simulated and proven.
- MATLAB is used to compare our two proposed protocols in terms of protocol overhead.

2.3 D2D Related Activities by 3GPP

3GPP has introduced long term evolution (LTE) or E-UTRAN in its Release 8 which is the access part of the evolved packet system (EPS). EPS and E-UTRAN are the two basic subsystems of an LTE and LTE-A architecture. E-UTRAN is the access network of the LTE system which consist of evolved node base station (eNB) as a main entities for macro-cells and home evolved base stations (HeNBs) for the femto-cells and the UEs [17]. EPS is the latest evolution of the 3GPP core network architecture. It is the core network of the LTE system based upon internet protocol (IP) [18]. LTE uses orthogonal frequency fivision multiplexing access (OFDMA) technology for down-link and spatial carrier sense orthogonal frequency division multiple access (SC-OFDMA) for up-link. It supports both frequency division duplex (FDD), time division duplex (TDD) and half duplex FDD for same radio access technology. The LTE access network is simply a network of BS, eNB, generating a flat architecture [19].
LTE-A was introduced in Release 10 of 3GPP. The main focus of LTE-A is to achieve higher capacity. It provides a higher bit rates in a cost efficient way and at the same time, completely fulfill the requirements set by international telecommunication union (ITU) for international mobile telecommunication (IMT) advanced. The main new functionality introduced in LTE-A is carrier aggregation (CA), enhanced use of multi antenna techniques, D2D and support for relay nodes

[20].
5G is the next phase of mobile telecommunication standards beyond the 4th generation (4G) which is expected to be in use in 2020. 5G is an integration of several technologies, use cases and standards such as internet of things (IoT), broadcast like services and lifeline communication. D2D communication has been regarded as a part of 5G mobile communication technology in its Mobile and wireless communications enablers for the twenty-twenty information society (METIS) project [21]. METIS project develops D2D technology components applicable in emergency/public safety scenarios.

2.4 Related Research Work on D2D Protocol Design

D2D is an extremely interesting research topic due to its abilities to save energy, operate in disaster situations, work without/partial support from infrastructure [22] and provides advertising and other relevant information to the end user. 3GPP continues to work on developing new popular technology as D2D communications in different scenarios. In addition, a lot of scientific research workers and telecommunication organizations are interested in its improvement and operation process. Related works to D2D are addressed.
According to [23], the authors suggested two D2D service discovery protocols, reactive (so-called "on-demand" protocol) and proactive (so-called "always on" protocol). Both of these protocols are focused on D2D connection covered by BS. The main difference between these protocols represents a device that initiates D2D connection. In their scenario, by using reactive protocol the end user will start handshake process for D2D communication. The second type, proactive protocol represents the initiation of D2D communication from BS. In that case, BS periodically sends multicast discovery message to all end users. The general conclusion is that, reactive protocol is better if needed to use low D2D traffic. However, proactive protocol has better performance if many end users want to initiate D2D communication.
The authors in [24] represent a review of D2D communications in cellular network. In addition, they defined two main different types of connections, inbound and outbound. The main different between inbound and outbound D2D connec-

tions represents licensed and unlicensed network. They classified inbound communication into two subgroups as underlay and overlay. The main problems that they found in underlay were the power control and signal overlapping between D2D and cellular end users. On the other hand, overlay does not have interference problems, but spectral efficiency is less in compare with underlay type. Furthermore, outbound has two sub-classes, controlled and autonomous connections. However, those types of communication do not have the same issues as inbound. Since, outbound belongs unlicensed network, the main problem faced is uncontrolled connections with less control capability of Quality of Service (QoS).
The work in [3] has addressed security related issues and potential solutions in D2D. They have purposed security architecture and discuss security requirements and threats. The first step in D2D is to discover devices within its proximity and establish a communication. Security must be implemented before start to exchange information. Therefore the authors have proposed ProSe security architecture to protect the network connection and information. The authors have mentioned the different types of threats to the D2D communication. For example, eavesdropping, impersonate attack, active attack on traffic data, active attack on control data, denial of service attack and man in the middle attack. For the security purposes five different security features against attacks have been discussed. These functions are network access security, network domain security, user domain security, application domain security, visibility and configuration security.
The authors in [25] proposed a secure key establishment protocol between two mobile users in D2D. They have also investigated the security requirements and challenges for key agreement protocol. Their approached is based upon the Diffi-Hellman key agreement protocol and commitment scheme. The design details and security analysis of the proposed protocol were represented. They combined their proposed protocol with existing Wi-Fi direct protocol and implemented it in Android smartphone. In [22] the authors have proposed a security protocol for public safety scenario. They also showed the existence of trade off points between connectivity and the increased overhead added by security for different values of the system parameters.
The 3GPP organization created a several technical reports (TRs) for the future development work relevant to D2D communication. The one of the first stage was

to create all possible scenarios and use case diagrams from service aspect. Thus document TR22.803 [26] gives feasibility study for ProSe with 13 general use cases and 13 public safety scenarios. The main studies of LTE and LTE-A radio technology are specified in the 36th TR series done by 3GPP. The more specific part is discussed in TR36.803 [14] as LTE D2D communication with ProSe from radio aspects.

Chapter 3

Scenarios and Protocol Design

The Discovering process represents the primary task for D2D communication and it starts before initiating the communication between two UEs. In addition, discovery mechanism includes both neighbor and service discovery processes. In this chapter, 3GPP scenarios of D2D communication and our selected scenario for protocols design are presented.

3.1 3GPP Scenarios

TR23.703 [1] is specified technical solution as the second stage. It is based on the relevant requirements from the stage one (TR22.803). The main study represents the possible 3GPP technical solutions for architectural enhancements which ProSe is required. This TR contains 38 solutions as follows: 11 proposed covering ProSe discovery, 6 for communication, 11 for relays, 5 for identities, 3 with wireless local area network direct communication and 2 for configurations. Fig. 3.1 shows D2D scenarios which are explained in TR23.703. The first part of that figure, 1A represents a simple ad-hoc connection between two UEs in unlicensed network. However, it shows D2D communication without associating with BS. In 1B scenario, one UE is associated with the BS as a part of cellular network and the other UE is out of coverage. The third part, 1C gives similar scenario as a previous 1B. However, both UEs realize D2D communication while they are receiving cellular signal from the same BS, located in identical public land mobile

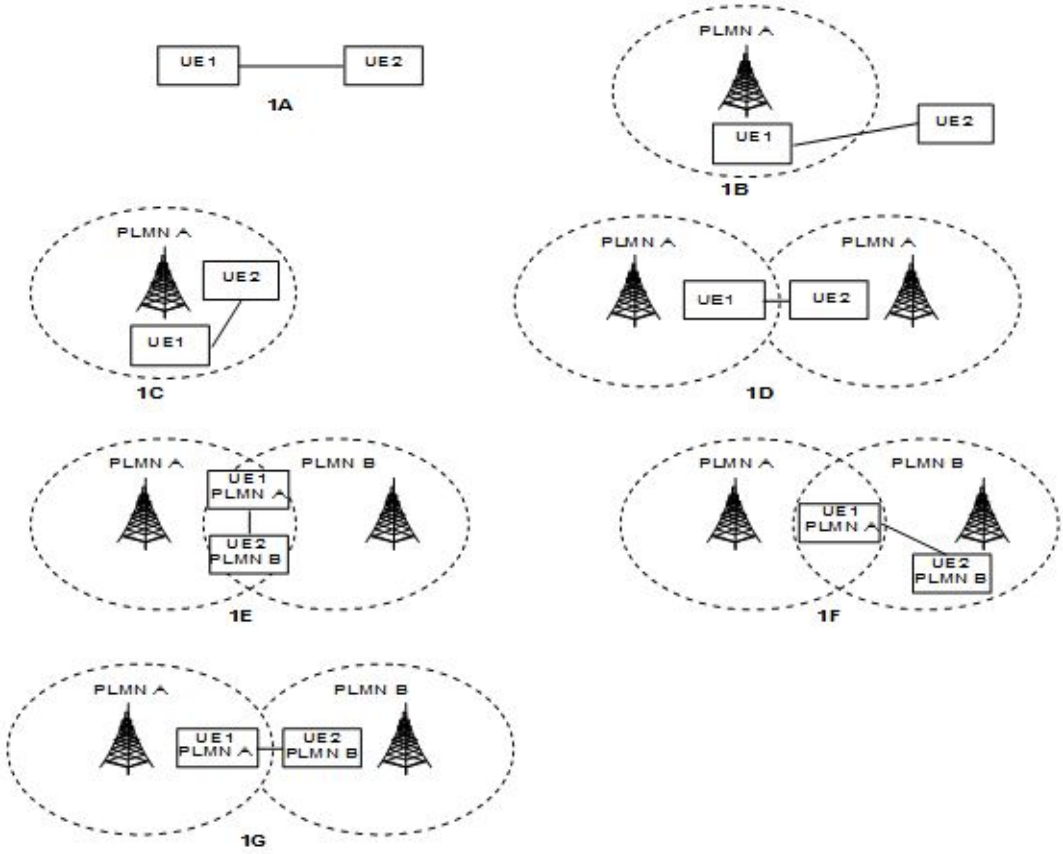


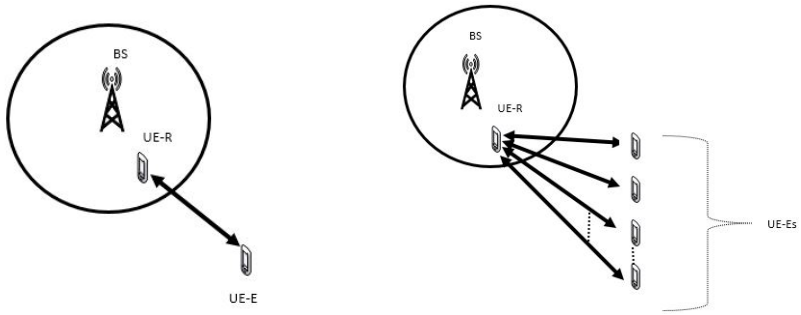
Figure 3.1: 3GPP D2D scenarios [1].

network (PLMN). In some of the situations, both UEs may detect D2D signal of each other even though they operate in the separate cells. In the other words, UEs are located inside coverage of the two different BSs from the same PLMN as situation 1D. The rest part of the mentioned figure, scenarios 1E, 1F and 1G represent D2D communication between UEs which operate in the separate PLMNs. Since, there are a lot of different mobile telecommunications operators, which operate together in the same area, their cellular signals may overlap. Specially, when UE acts on the edge of the cell, it may receive signal from the other PLMN. The part 1E shows that UEs receive cellular signal from the both BSs which belong to the different PLMNs. The next scenario, 1F is similar as previous one. The main difference is that only one UE receives the signal from the both BSs, while BSs do

not belong to the common PLMN. The last possible 3GPP scenario represents two UEs in the cooperation with separate BSs in the different PLMNs. Anyway, UEs are located in the proximity area for establishing D2D connection. 3GPP scenario 1B is selected as the basic scenario in our protocol design.

3.2 Our Selected Scenarios

Fig. 3.2a and Fig. 3.2b show possible situations for proposed protocols design where BS cooperates with UE-R which is inside coverage area. Here, UE-R must respect a role of the cellular network as others UEs. Further, the selected scenario is divided into two parts: primary and secondary. Primary scenario consists of only one UE-R and one UE-E as shown in Fig. 3.2a. Secondary scenario contains one UE-R and multiple UE-Es as shown in Fig. 3.2b. For simplicity, the primary scenario is considered for proposed protocols design. However, proposed protocols are equally applicable for secondary scenario too. In addition, before discovery process starts, UE's ProSe registration process is already performed.



(a) (b)

Figure 3.2: (a) Primary scenario: one UE-E outside and one UE-R inside coverage and (b) Secondary scenario: multiple UE-Es outside and one UE-R inside coverage.

3.3 Reactive Protocol Design

Proposed reactive protocol is based on the primary scenario where UEs are willing to be discovered for D2D communication. First, UE-E initiates discovery process by sending a discovery message to UE-R. The discovery message includes UE-R's identity and type of the required service. Connection between them is directly as one-to-one. With reactive protocol, D2D initiation process is started only when UE-E requires ProSe. Otherwise, D2D connection is closed. Such type of D2D communication is called PULL mechanism. Since, UE-E is outside of coverage area, BS does not exchange any handshake messages with it. UE-R plays a role as relay to forward all detail information about UE-E to BS. According to the information which are received from UE-R, BS and AS check the authenticity and authorization of UE-E for using ProSe. Therefore, BS does not apply any role for the D2D discovery process. If UE-E is satisfied all the requirements for ProSe, then steps of delivering service information should be continued. Our proposed protocol as shown in Fig. 3.3 is divided into two phases, neighbor and service discovery phase and ongoing D2D communication. In the first phase, the total number of handshake messages is six. In ongoing D2D communication section, the total number of exchanged messages is also six. In the showed protocol design, the last three handshake messages are used for the D2D termination process. The total number of ProSe handshake messages by using reactive protocol is fifteen. All those fifteen messages are considered for calculation of the protocol overhead, which is discussed in Chap. 4. The main required steps for neighbor and service discovery process are described as follows:
Neighbor and service discovery phase:

- Step 1: UE-E sends *"Discovery signal"* to UE-R. *"Discovery signal"* contains source ID, destination ID, type of required service, location of UE-E.
- Step 2: UE-R calculates distance between UE-R and UE-E, delay, signal quality, SINR, and interference. UE-R forwards all these information to BS and asks for permission to establish D2D connection and to deliver requested services to UE-E.
- Step 3: BS checks the authority of UE-E. If it is authorized, then BS asks

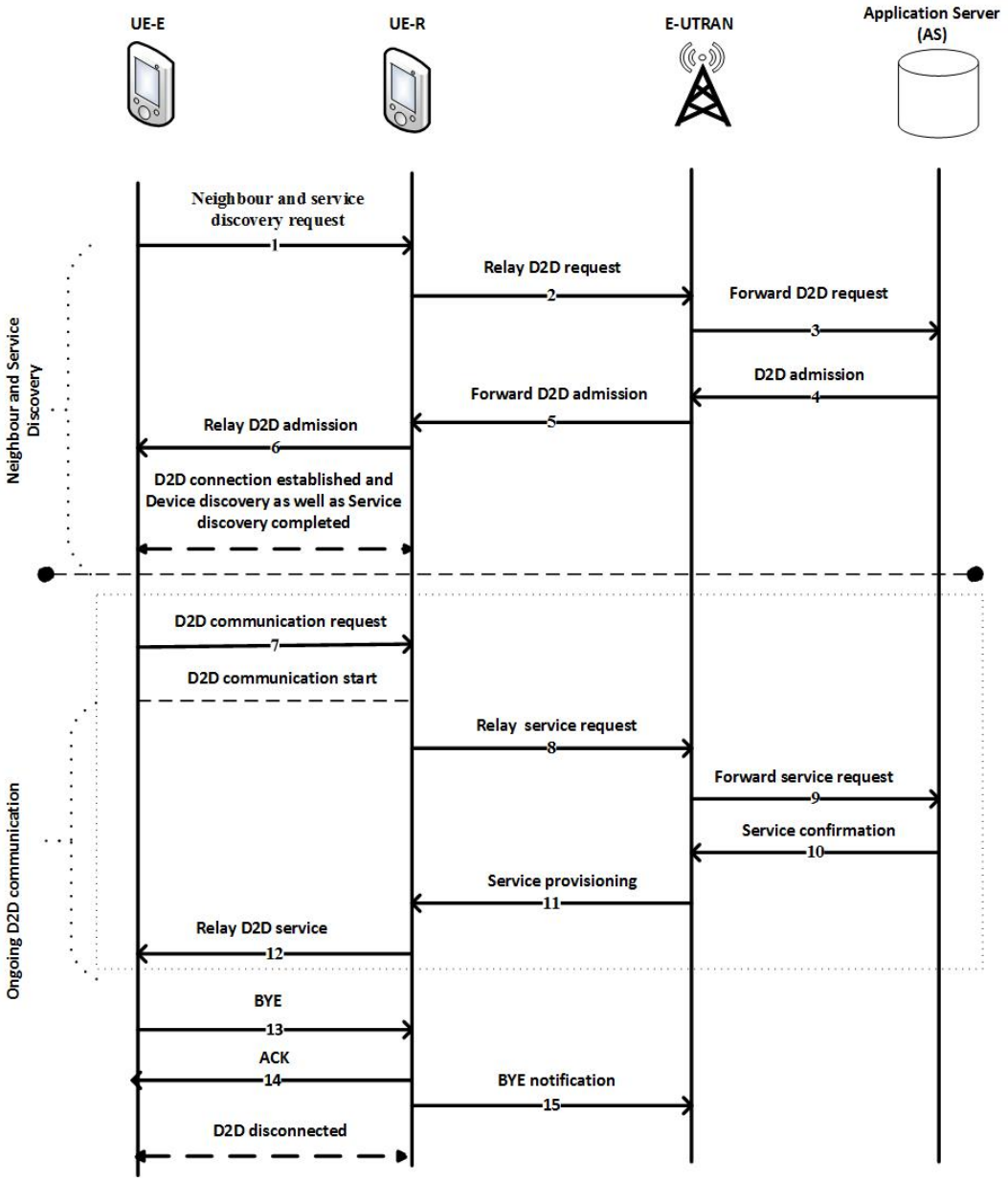


Figure 3.3: Discovery process using reactive protocol.

AS for the availability of services. Otherwise, BS replies with negative response to UE-R.

- Step 4: AS checks availability of services and responses positive, if it has services requested by UE-E. Otherwise it sends negative response to BS.

- Step 5: BS sends positive response to UE-R, if it received positive response from AS.
- Step 6: UE-R relays to UE-E the response of BS.
- Step 7: UE-E sends *"D2D communication request"* in order to access the services.

Ongoing D2D communication phase:

- Step 8: UE-R sends *"Relays services request"* to BS.
- Step 9: BS asks AS to provide the services.
- Step 10: AS provides the services information to BS.
- Step 11: BS forwards the services information to UE-R.
- Step 12: UE-R relays the services provided by BS. The steps from 9 to 12 are continued until either UE-R or UE-E terminates D2D communication.
- Step 13: UE-E sends *"BYE"* messages to UE-R.
- Step 14: UE-R sends *"ACK"*.
- Step 15: UE-R relays *"BYE"* messages to BS. D2D connection is now disconnected.

3.4 Proactive Protocol Design

In proactive protocol, UE-R does not wait for UE-E(s) to start D2D communication as with reactive protocol. UE-R relays the services advertisement information from BS. Any interested UE-E(s) response to this message. During the device discovery process, the type of communication between UE-R and UE-Es is multicast. However, after completion of D2D discovery process between them, they exchange unicast messages. Also, D2D connection between UE-R and UE-E is initiated even though UE-E does not require specific service information. Such type is called PUSH mechanism.Proactive protocol is very useful for commercial

companies, who want to promote and provide information about themselves to the customers. The proposed proactive protocol design is divided into thirteen steps also with two phases. Fig3.4 represents proposed primary scenario for proactive

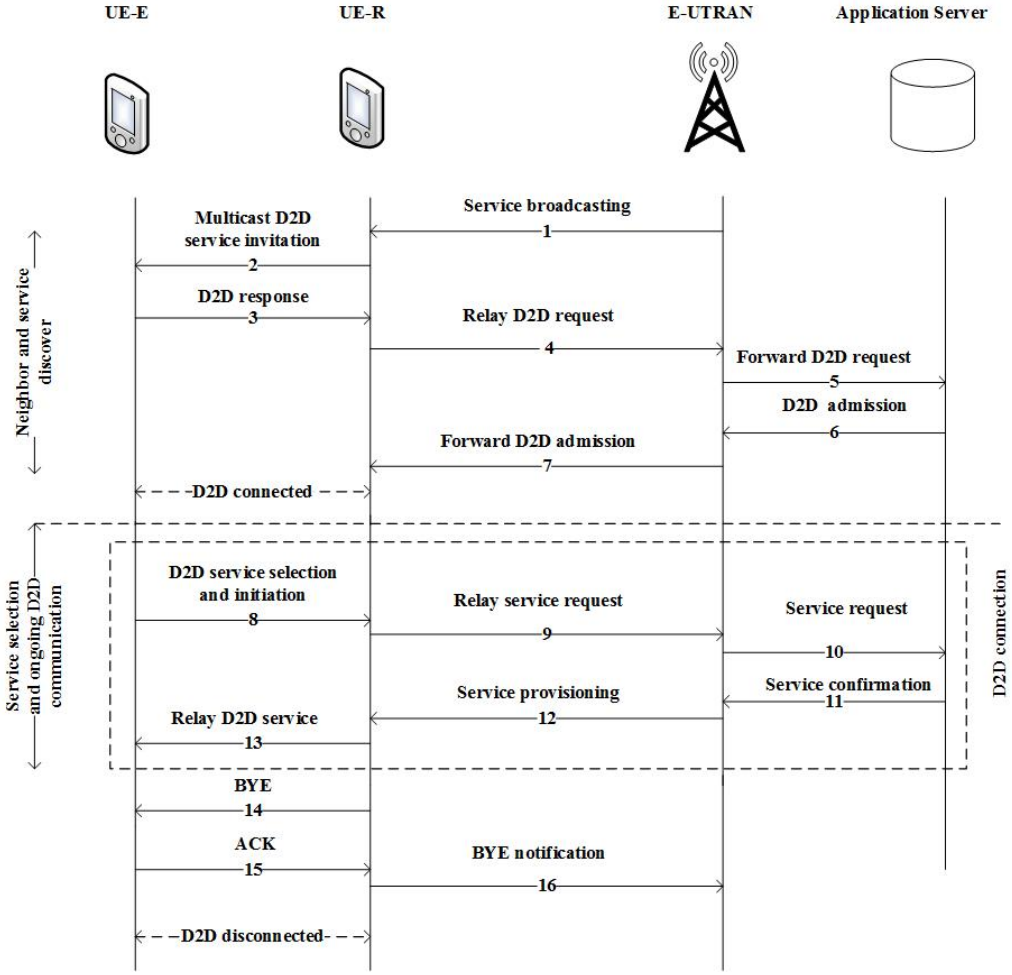


Figure 3.4: Discovery process using proactive protocol.

protocol design with handshake processes as follows:
Neighbor and service discovery phase:

- Step 1: BS suggests *"Service advertisement"* to UEs in its coverage by using broadcast message.
- Step 2: UE-R as a relay device sends *"Multicast D2D service invitation"* to the proximity UE-E(s). Multicast message contains its ID and type of the

service information.

- Step 3: UE-E replies with unicast *"D2D response"* message to UE-R as acceptance of service invitation.
- Step 4: UE-R asks BS for D2D request permission by sending information about UE-E.
- Steps 5, 6 and 7: represent D2D checking processes for UE-E. BS sends to AS *"Forwards D2D request"*. Afterwards, AS saves the information about UE-E in its database and checks channel capacity for it. After this procedure, AS answers on UE-R's request by sending *"D2D admission"* message via BS.

Service selection and ongoing D2D communication phase:

- Step 8: UE-E chooses the specific service that is interested by sending *"D2D service selection and invitation"* to UE-R.
- Step 9: UE-R forwards service request to BS.
- Steps 10, 11 and 12: represent the service provisioning phase from BS to UE-R. It requires service checking and confirmation from AS, with processing and distributing the requested service information.
- Step 13: UE-R delivers *"Relay D2D service"* information by unicast messages.

3.5 Chapter Summary

This chapter has discussed about the different D2D scenarios suggested by 3GPP and the scenario we selected for protocol design. We selected the scenario 1B as suggested by 3GPP where one UE is located outside coverage area. The scenario is further divided into primary and secondary. The primary scenario is based on one UE-E and one UE-R and secondary scenario is depend on one UE-R and multiple UE-Es. We proposed the neighbor and service discovery protocols, reactive

and proactive for given scenarios. In the reactive protocol UE-E initiates the discovery process where as in proactive UE-R initiates the discovery process after receiving service broadcast message from BS. The total number of messages exchanged in reactive protocol are 15 where as in proactive protocol the number is 16. In case of proactive, UE-R always multicast the discovery request even though if it does not receive response from UE-E(s).

Table 3.1: Difference between reactive and proactive protocols

	Reactive protocol	*Proactive protocol*
Announcing/Monitoring	UE-E/UE-R	UE-R/UE-E
Communicaiton	Unicast	Multicast during discovery process and unicast during communication process
Number of exchanged messages	15	14+2 (one broadcast and one multicast discovery message)

Chapter 4

Protocol Implementation and Validation

This chapter describes the implementation and validation of proposed reactive and proactive protocols. The implementation and validation processes are based on primary design. Also, the calculation and comparison of proactive and reactive protocols overhead are shown below.

4.1 Protocol Implementation using SDL

4.1.1 SDL implementation from UE-E's prospective

With reactive protocol, D2D connection is initiated from UE-E's side. Therefore, implementation process starts from the same position. Fig. 4.1 and Fig. 4.2 show the SDL diagrams and illustrate of exchanging messages from the UE-E's perspective by using reactive and proactive protocols. On the following figures, the shown numbers are associated with the numbers of the handshake messages from the proposed protocol design graphs. Considering that UE-E has D2D communication channel only with UE-R, their handshake messages are described as follows:

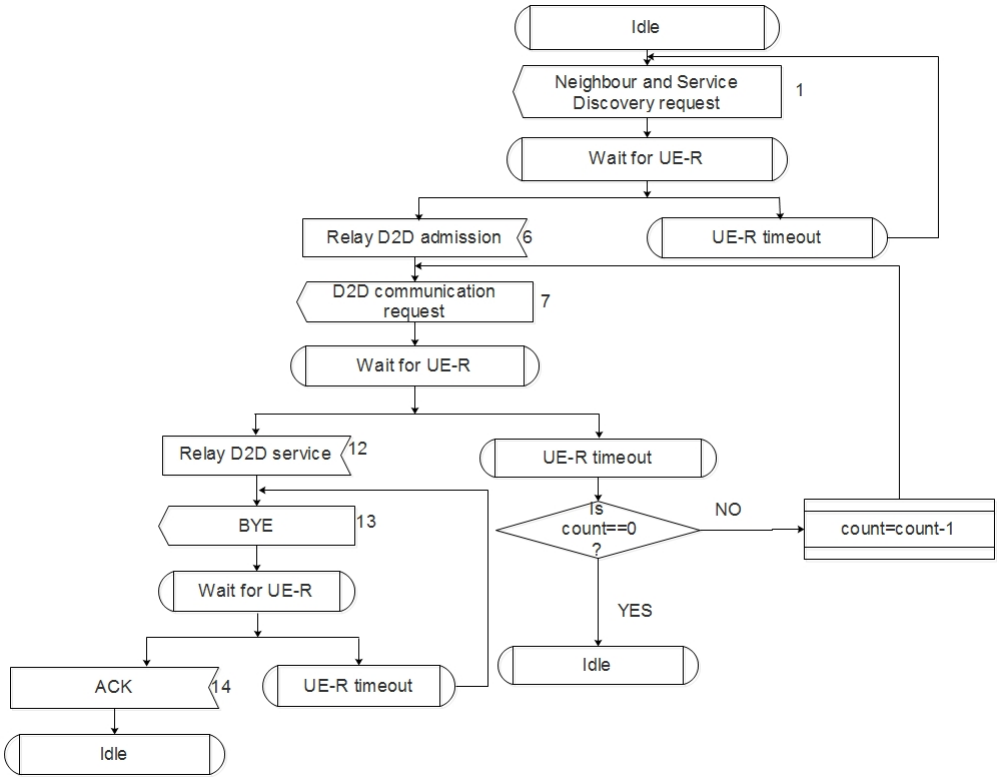


Figure 4.1: SDL diagram from UE-E for reactive protocol.

- UE-E sends *"Neighbor and Discovery request"* signal to UE-R as message 1.
- During timeout period, UE-E waits for UE-R reply. After timeout period, if UE-R does not answer on request, UE-E repeats the same request.
- UE-E receives *"Relay D2D admission"* from UE-R as message 6.
- In order to access service information, UE-E sends *"D2D communication request"* as message 7.
- For the time out period UE-E waits for *"Relay D2D service"*, message 12. If it does not get any answer, UE-E repeats the same message several times until timeout counter become null.

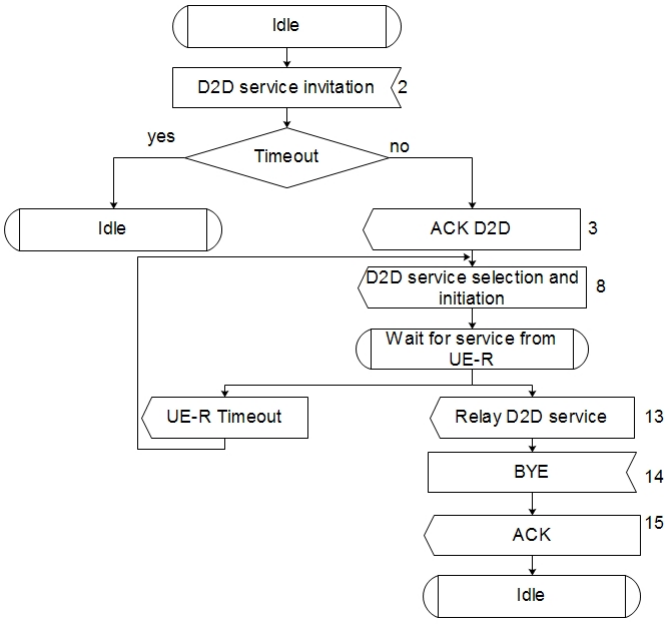


Figure 4.2: SDL diagram from UE-E for proactive protocol.

- UE-E sends *"BYE"* in message 13 for termination the D2D communication with UE-R.
- UE-E receives *"ACK"* as confirmation of ending the communication.

The description of SDL implementation from UE-E's prospective for proactive protocol is similar to SDL implementation of reactive protocol. However, in the case of using proactive protocol, UE-E starts D2D communication process by receiving initiation message from UE-R.

4.1.2 SDL implementation from UE-R's prospective

Fig. 4.3 and Fig. 4.4 show the SDL diagrams from the point of view of UE-R for reactive and proactive protocols respectively. The shown messages are exchanged between UE-R with its neighbors UE-E and BS by using reactive protocol as follows:

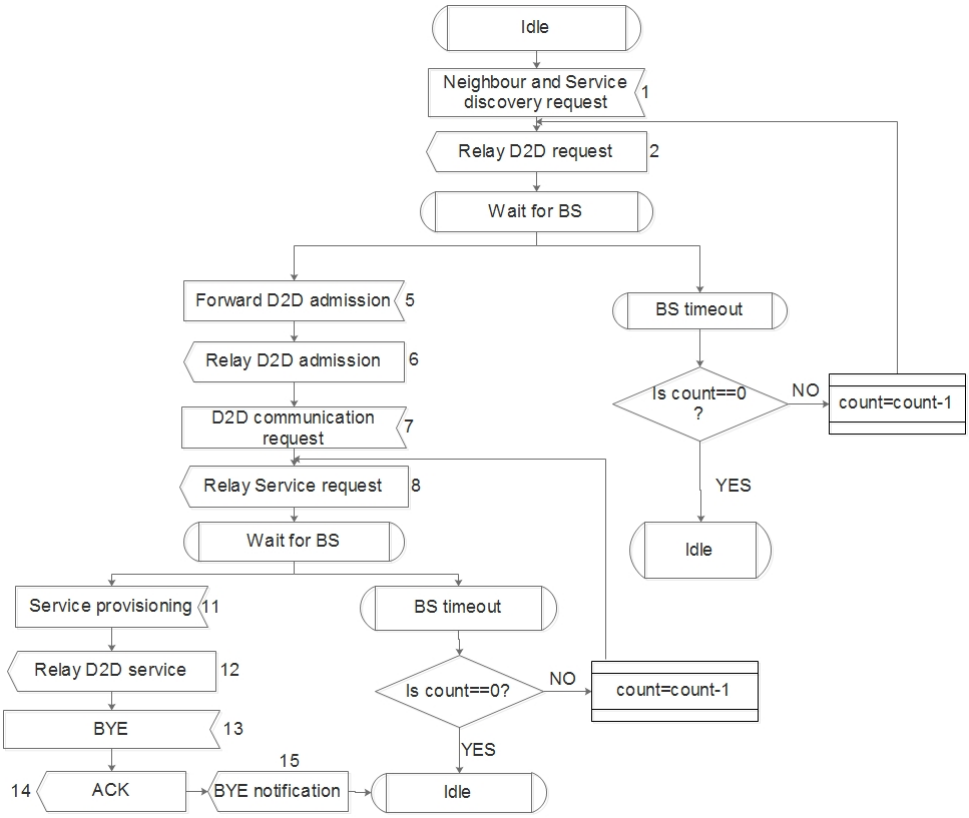


Figure 4.3: SDL diagram from UE-R for reactive protocol.

- UE-R receives *"Neighbor and Discovery request"* from UE-E as message 1.
- In order to ask for D2D communication permission, UE-R sends *"Relay D2D request"* to BS (message 2). If UE-R does not receive any answer from BS, it repeats the same request.
- UE-R receives *"Forward D2D admission"* from BS (message 5).
- UE-R sends *"Relay D2D admission"* to UE-E as message 6.
- UE-R receives *"D2D communication request"* from UE-E (message 7).
- In order to get service information, UE-R sends *"Relay service request"* to BS as message 8.

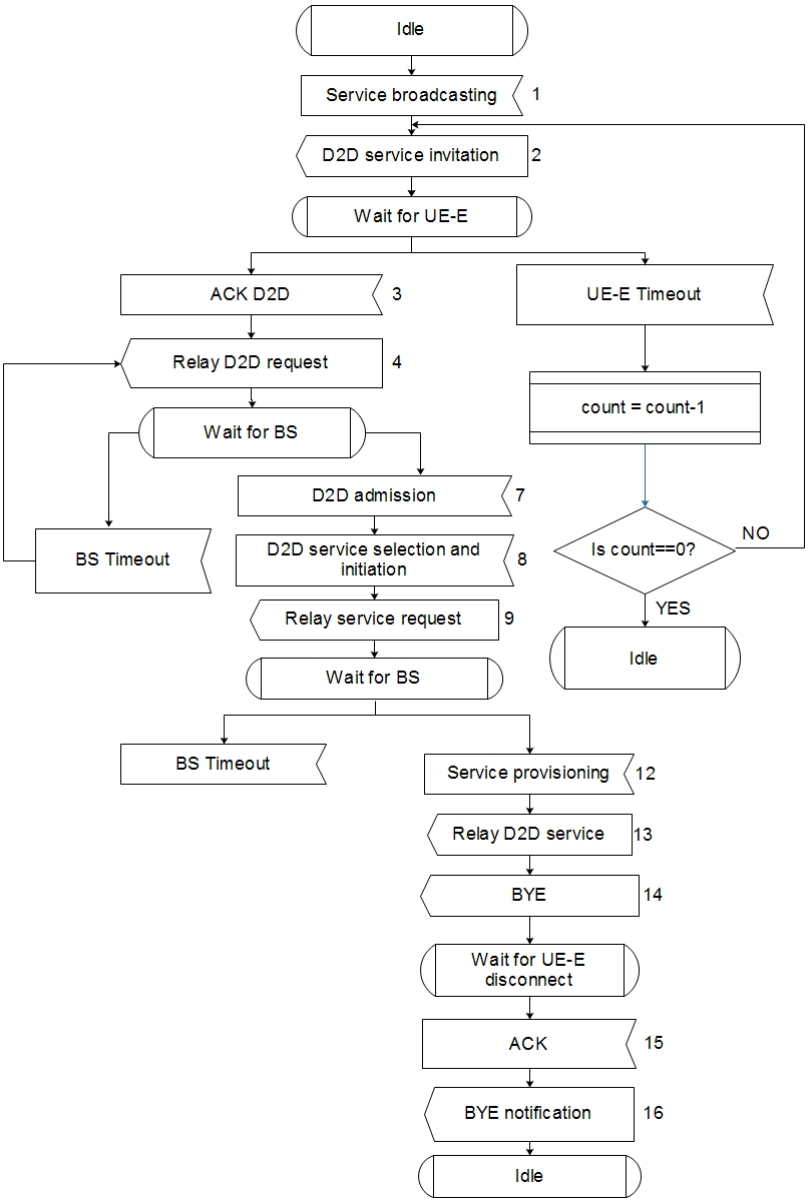


Figure 4.4: SDL diagram from UE-R for proactive protocol.

- During timeout period, UE-R receives *"Service provisioning"* message from BS. If UE-R does not receive service information, it repeats its request several times until counter is active.
- UE-R forwards *"Relay D2D service"* to UE-E and delivers service infor-

mation to UE-E (message 12).

- For termination process of D2D connection, UE-R receives *"BYE"* from UE-E as message 13.
- Messages 14 and 15, *"ACK"* and *"BYE notification"* are sent from UE-R to inform UE-E and BS that D2D communication is terminated.

By using proactive protocol the SDL implementation from UE-R's point of view represents receiving broadcast message from the BS as a first step. In this case, UE-R sends multicast *"D2D service invitation"* message to its neighbors UE-Es. The rest of SDL implementation steps are the similar as the SDL implementation of reactive protocol design.

4.1.3 SDL implementation from BS's prospective

Fig. 4.5 and Fig. 4.6 show the SDL diagrams from the point of BS's view for reactive and proactive protocol respectively. Messages that BS exchanges with UE-R and AS as its neighbor devices by using reactive protocol are described as follows:

- BS receives *"Relay D2D request"* from UE-R as message 2.
- After processing time, BS sends *"Forward D2D request"* to AS (message 3). During timeout period, BS receives *"D2D admission"* from AS (message 4). Otherwise, BS repeats same request.
- BS establishes communication with UE-R by sending message 9 (*"Forward D2D admission"*).
- By receiving *"Relay service request"* from UE-R, BS forwards the same request to AS as *"Forward service request"* (message 10).
- BS receives *"Service confirmation"* from AS and forwards it to UE-R as *"Service provisioning"*, messages 11 and 12. Unless, if BS does not receive the answer from AS, it repeats message 10 several times until counter is active. Otherwise, BS goes in idle state.

- After completion provisioning of D2D service, BS receives *"BYE notification"* from UE-R as message 16.

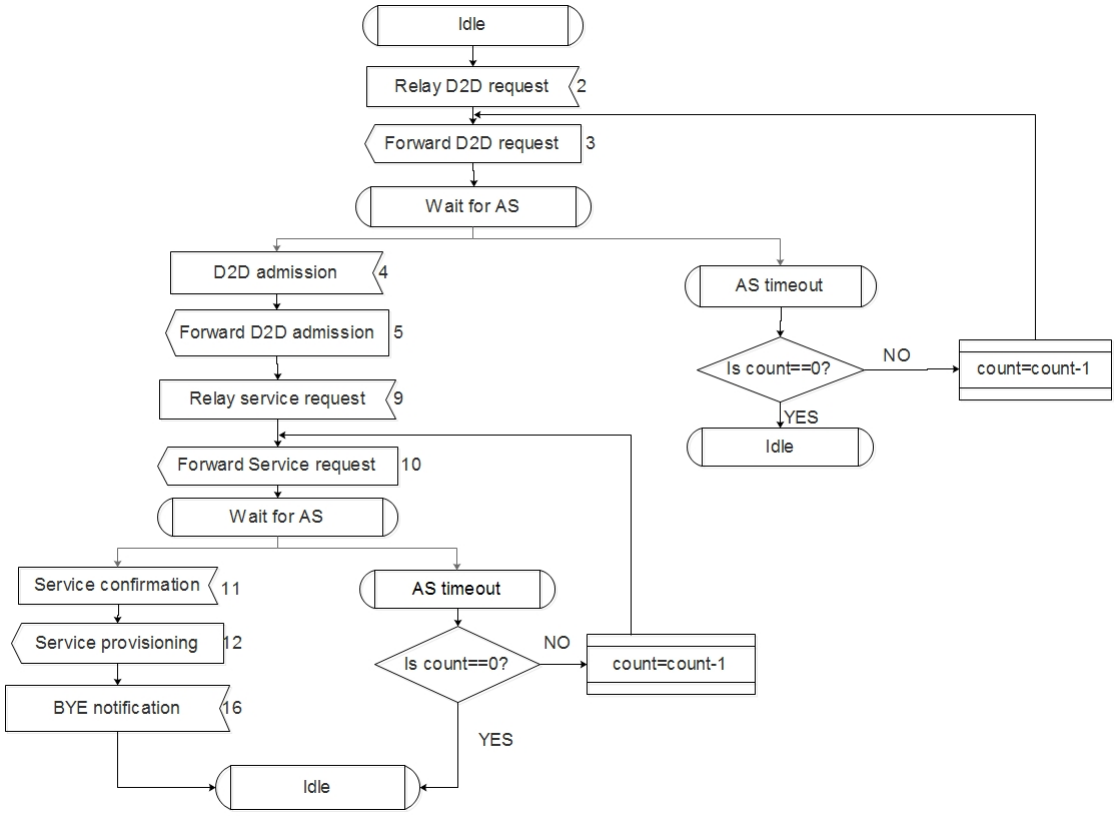


Figure 4.5: SDL diagram from BS for reactive protocol.

4.1.4 SDL implementation from AS's prospective

Fig. 4.7a and Fig. 4.7b show the SDL diagrams from the point of view of AS for reactive and proactive protocol respectively. The messages exchange between AS and BS for reactive protocol are as follows:

- AS receives *"Forward D2D request"* as message 3.

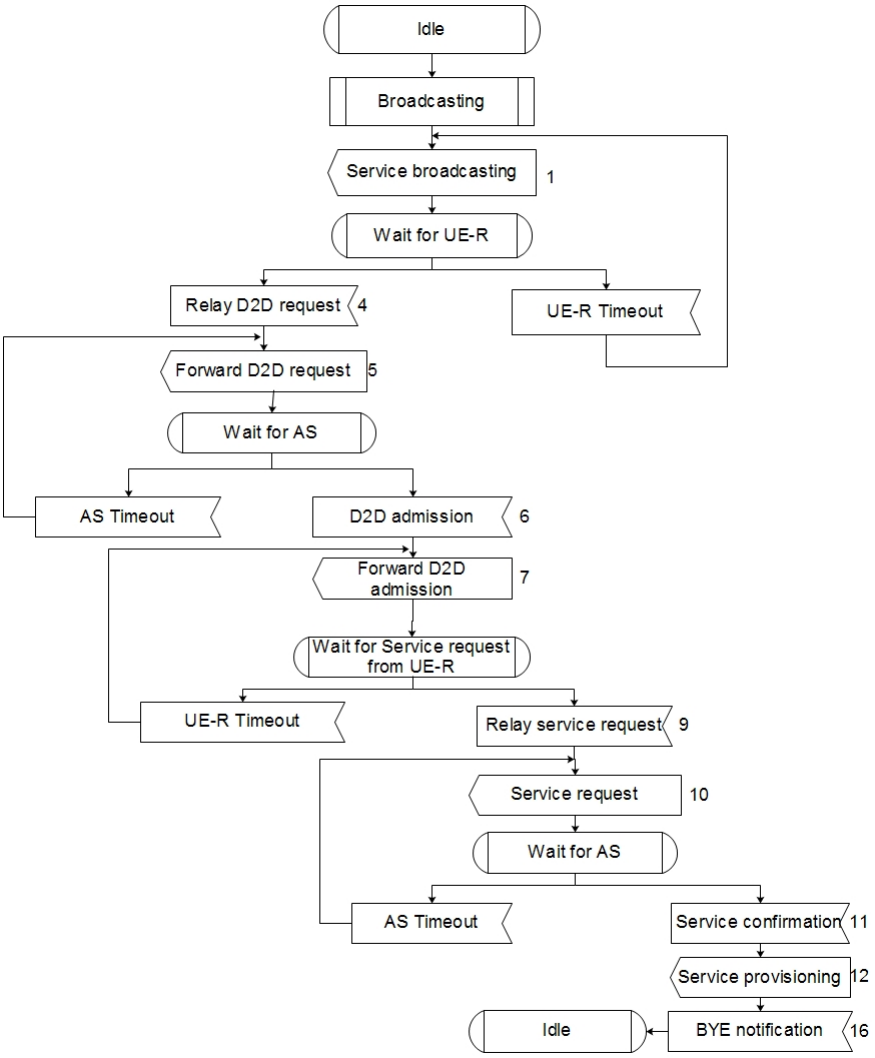
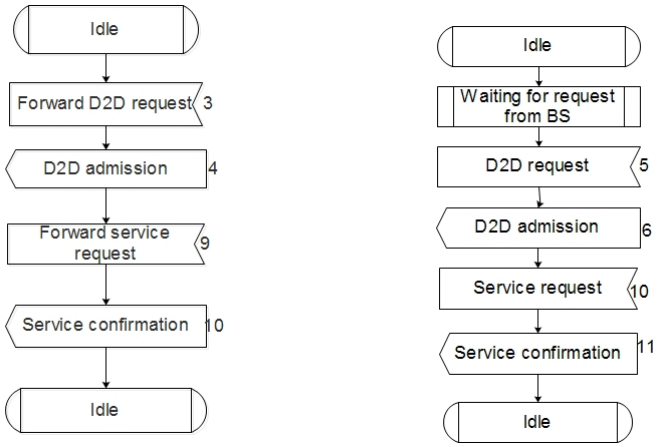


Figure 4.6: SDL diagram from BS for proactive protocol.

- After processing time, AS replays to BS by sending *"D2D admission"* (message 4).
- AS receives from BS *"Forward service request"* as message 9.
- AS sends *"Service confirmation"* as message 10 to BS.



(a) (b)

Figure 4.7: SDL diagram form AS's prospective for (a) Reactive protocol and (b) Proactive protocol.

4.2 Protocol Validation using SPIN

In order to validate the proposed protocols, it is necessary to simulate them. In this section, two different SPIN output as simulate and verification are represented.

(i) SPIN simulate output for reactive and proactive protocol Fig. 4.8 and Fig. 4.9 illustrate SPIN simulate output for reactive and proactive protocol respectively. These diagrams represent exchanging handshake messages between UE-E, UE-R, BS and AS during D2D neighbor and service discovery process. In the figures below, EndUser represents UE-E, RealyUser represents UE-R, BaseStation represents BS and AppServer represents AS. Those graphs show exchanging handshake messages without "black hole". In other words, proposed reactive and proactive protocols work constantly without loop.

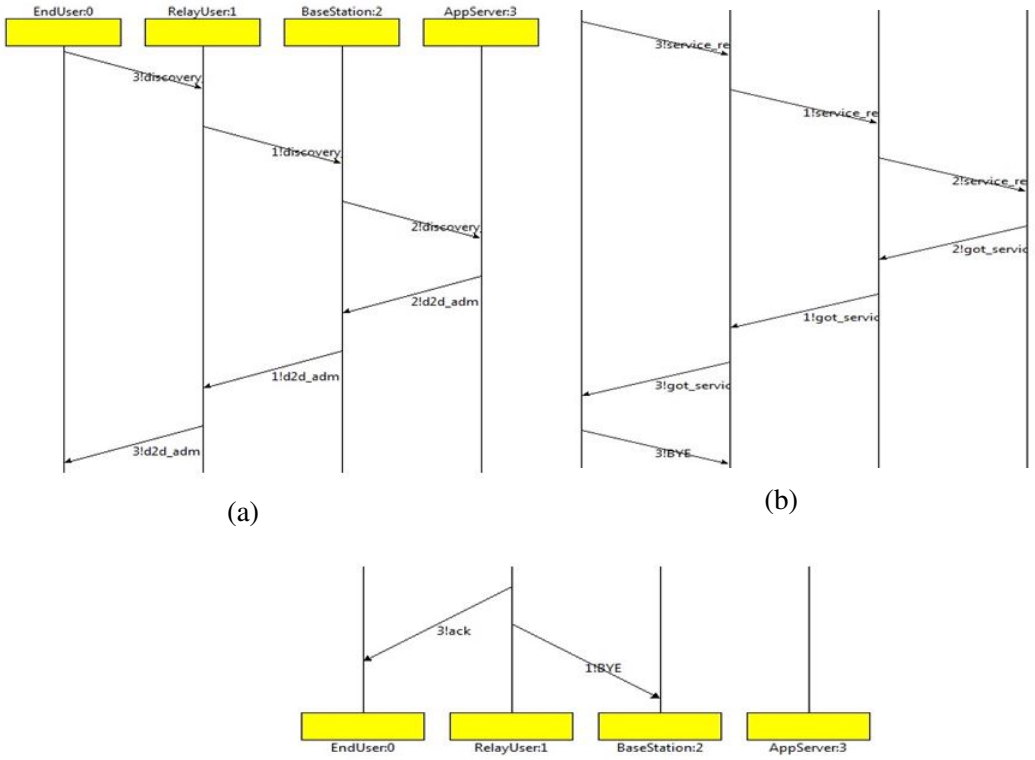


Figure 4.8: SPIN simulate output for reactive protocol.

The meaning of the messages exchanged among UE-E, UE-R, BS and AS are described as follows:

- "$discovery\_req$" message is sent by UE-E to UE-R as neighbor and service discovery message which UE-R relays to BS and BS forward to AS.
- "$d2d\_adm$" is message from AS as a response of "$discovery\_req$" message.
- "$service\_req$" and "$serv\_req$" is a service discovery message for reactive and proactive protocol respectively.
- "got_ser" and "$serv\_conf$" is reply from AS as a response of "$service\_req$" and "$serv\_req$" respectively which UE-R relays to UE-E for reactive and proactive protocol respectively.

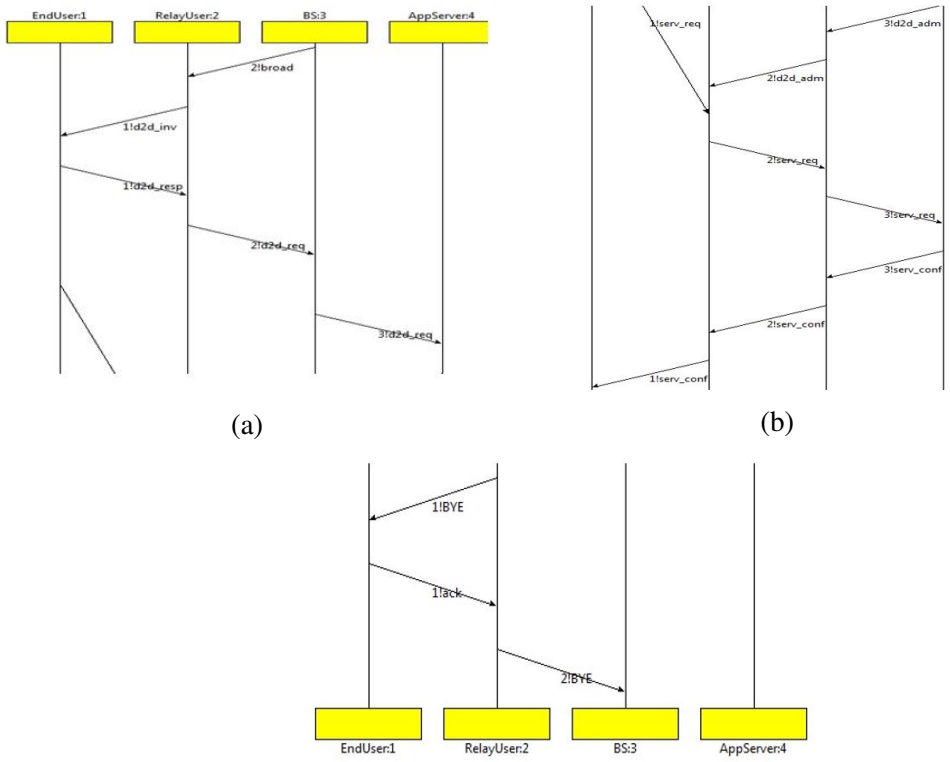


Figure 4.9: SPIN simulate output for proactive protocol.

- "BYE" is for termination of connection.
- "ack" is acknowledgment of "BYE" message.
- "$broad$" is broadcast service message sent by BS to all UE-Rs in proactive protocol.
- "$d2d\_inv$" is multicast service message sent by UE-R.
- "$d2d\_resp$" is neighbor and service discovery message as response of "$d2d\_inv$".
- "$d2d\_req$" is D2D request message send by UE-R to BS at the instance of UE-E.

(ii) SPIN verification output for reactive and proactive protocol
The verification of reactive and proactive protocols is shown in Fig. 4.10. represents validation output of reactive protocol and it is reached 35 states

as the longest depth state without errors. Moreover, validation output of proactive protocol is shown in the Fig. 4.11. That protocol is reached the longest depth position of 42 states, also without errors. The full simulation of a global system state required 35 bytes of memory per every state for reactive and 44 bytes for proactive protocol. With those validation output parameters of the proposed protocols, reactive and proactive are designed and simulated to work without errors.

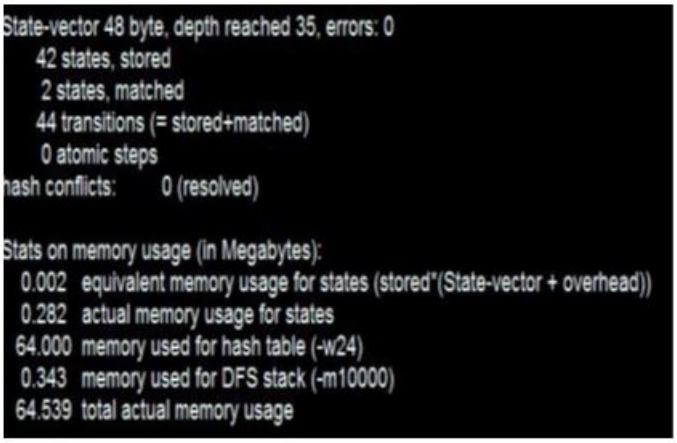


Figure 4.10: SPIN verification output for reactive protocol.

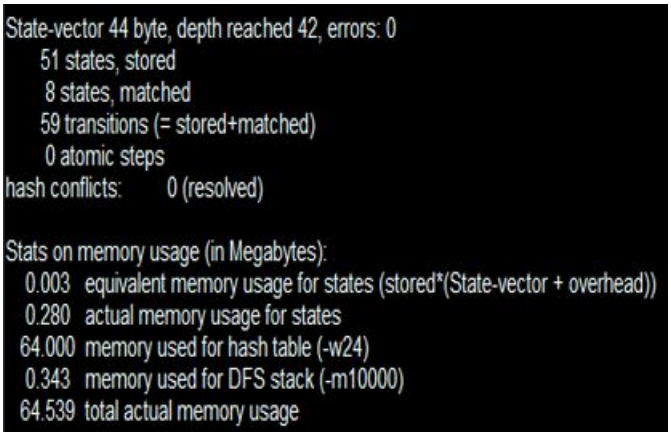


Figure 4.11: SPIN verification output for proactive protocol

4.3 Protocol Overhead Comparison

4.3.1 Spatial distribution of UE-Es

Before proceeding of the protocol overhead calculation for the different cases of D2D request, it is important to analyze the behavior of UE-E. In other words, how UE-Es are distributed and what is the probability for occurrence at least k numbers of D2D request within a given distance. As shown in Fig. 4.12, UE-Es are randomly distributed according to the Poisson point process, which represents the most important model for random point pattern [27]. In addition, assume that the position of UE-R is fixed for BS. In Fig. 4.12, O is the center of the cell where

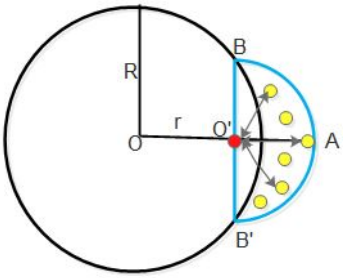


Figure 4.12: Spatial distribution of UE-Es outside of coverage area.

BS is located, O' is the point where UE-R is located, which is r distance far from BS. It is assumed that there are total N number of UE-Es which are randomly distributed within area S and proximity distance D from UE-R. Among N UE-Es, only n UE-E(s) want to have D2D communication with UE-R. In our scenario UE-R located inside coverage area, so that it covers UEs, which located inside and outside cell coverage. However, we are not considering UEs inside cell coverage area. Therefore, we should calculate the user density outside coverage area . The UE-E density within area S is calculated as follows [27]:

$$\lambda = \frac{N}{S} \tag{4.1}$$

As shown in Fig. 4.13, S is calculated by subtracting shaded area s from semi circle area $S^{'}$ having radius $R^{'}$.

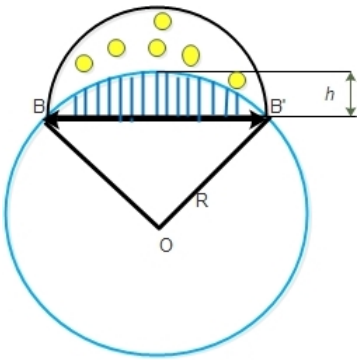


Figure 4.13: UE-Es density calculation.

$$S = S^{'} - s \tag{4.2}$$

$$S^{'} = \pi \times R'^{2} \tag{4.3}$$

Area of shaded portion is calculated as follows [28]:

$$s = R^2 \times \cos^{-1}(\frac{R-h}{R}) - (R-h)\sqrt{(2R \times h - h^2} \tag{4.4}$$

where h is the height of the shaded arced portion and R is the radius of network coverages cell.
UE-R and UE-E form a D2D pair if and only if the distance d between them is less than or equal to targeted distance D. The probability that the nearest distance between two UEs forming the D2D pair is shorter than or equal to the targeted distance D meter(s) within a given area is calculated as follows [27]:

$$P(d \leqslant D) = 1 - e^{-\lambda \times pi \times D^2} \tag{4.5}$$

Fig. 4.14 explains that UE-R has at least k number of UE-E(s) as its nearest neighbor within D meter(s). Assume that is selected n number of UE-E(s) among N UE-E(s). In interval of n UE-E(s), UE-R should have at least k number of nearest neighbor UE-E(s) which is located in D meter(s) away from UE-R. These k UE-E(s) forms the D2D pair(s) with UE-R. To find out the k success out of n

observations, binomial distribution is used as [27]:

$$P(k) = 1 - \sum_{i=0}^{\infty} \binom{n}{i} (1-p)^i p^{(n-i)} \tag{4.6}$$

where p is the probability without nearest neighbor within distance D and calculated as:

$$p = 1 - P(d \leqslant D) \tag{4.7}$$

Fig. 4.14 shows that when transmission distance D increasing, the probability of

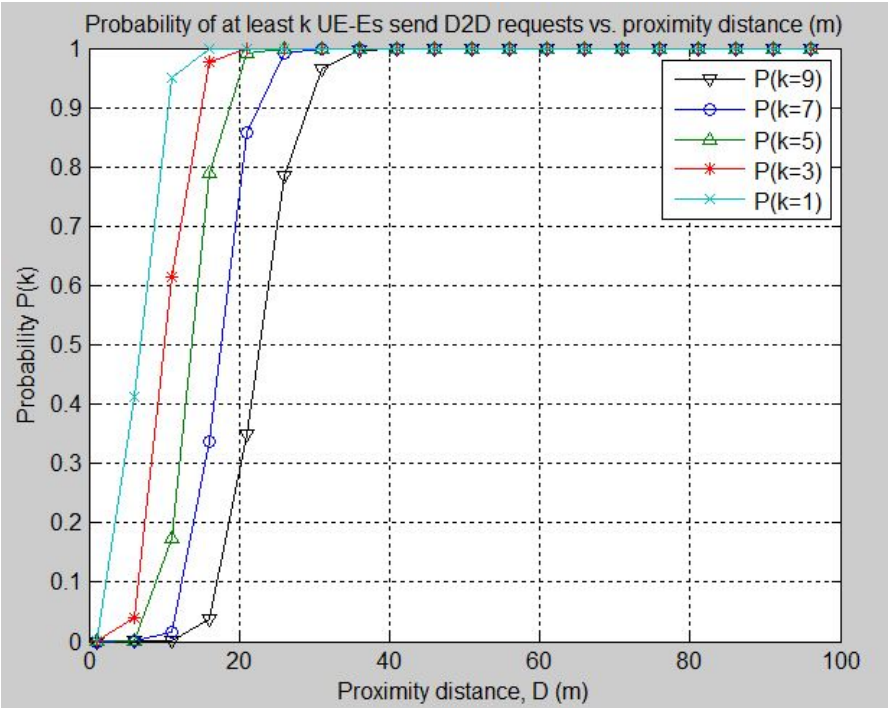


Figure 4.14: Probability function for random distribution of UE-Es.

having UE-E(s) in UE-R's proximity increases too. If more UE-Es are in neighborhood of UE-R, there is the high probability that at least k UE-E(s) may make the D2D pair with UE-R.

4.3.2 Case I : Same number of requests occurs at each timeslot

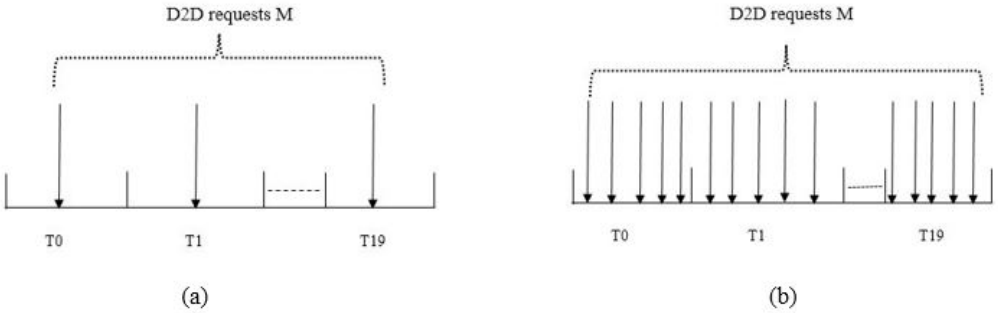


Figure 4.15: Same number of requests per timeslot.

Fig. 4.15 explains our case I, which deals with the condition when there is the same number of D2D requests at each timeslot. First consider the case where the total number of the D2D request is one at each timeslot and second case when the total number of the D2D request is more than one. For the calculation of the second condition is assumed that the number of D2D request is five. The control overhead for proactive and reactive protocol is calculated as in equations 4.8 and 4.9.

$$CO_p = \frac{T' \times (2 + (14 \times M)) + (2 \times (T - T')}{T} \tag{4.8}$$

$$CO_r = \frac{T' \times 15 \times M}{T} \tag{4.9}$$

Result of case I

The network parameters for calculation of protocol overhead for both proactive and reactive protocols are described in Tab. 4.1. Fig. **??** shows the comparison between reactive and proactive protocols in terms of protocol overhead where number of D2D requests at each timeslot is fixed.

Table 4.1: Network parameters configuration to calculate control overhead for case I

Parameters	*Symbols*	*Values*
Total number of UE-Es.	N	15
Number of UE-Es participating in D2D communication.	n	10
Total timeslots.	T	20
Timeslots where D2D request occurs	T'	1 to T
D2D request at each timeslots	M	1 and 5

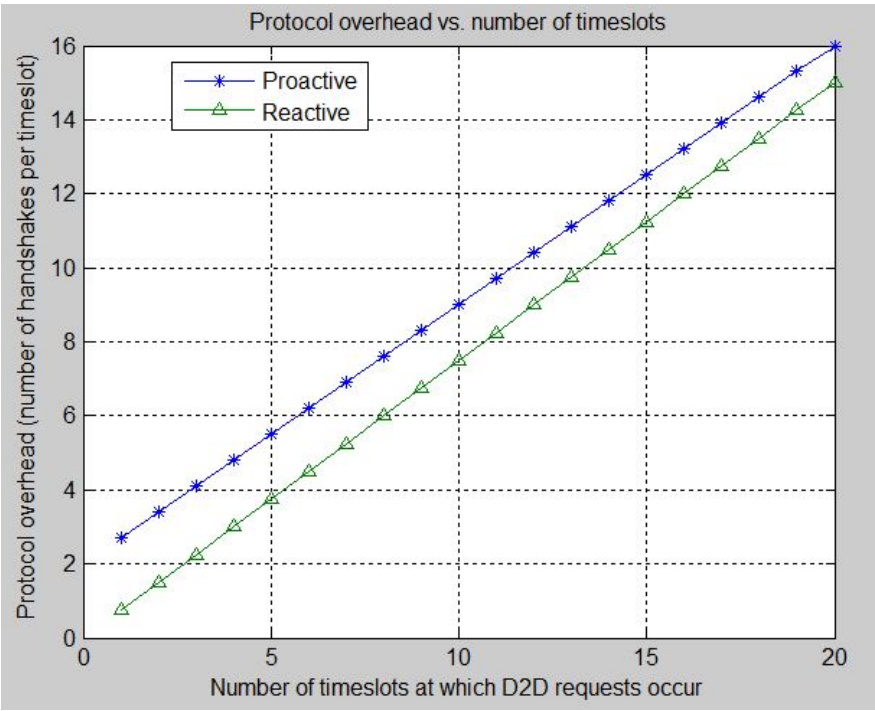


Figure 4.16: Protocol overhead vs. number of timeslots when M = 1.

From Fig. 4.16 it is clear that when number of D2D request is one, reactive protocol is better to select because protocol overhead for reactive protocol is relatively less in comparison to proactive protocol which has relatively more overhead. Therefore, reactive protocol is better choice for unicast communication. Fig. 4.17 is the graph between protocol overhead and timeslot when D2D re-

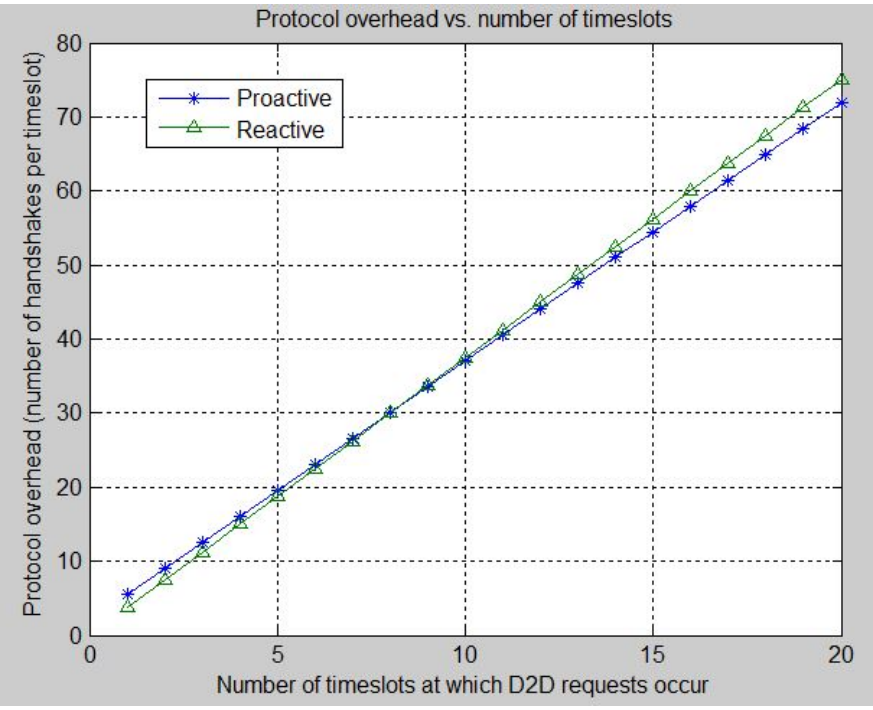


Figure 4.17: Protocol overhead vs. number of timeslots when M = 5.

quests at each timeslot is five. From graph, we can see that until timeslot five reactive protocol is better than proactive protocol because reactive protocol has less overhead than proactive protocol. From timslot five to timeslot twelve, both protocol has almost same overhead. After timeslot twelve, proactive protocol has less overhead than reactive overhead. Therefore, we can conclude from above graph that it is better to choose proactive protocol when there is relatively high number D2D requests at each timeslot and overall high number of D2D requests in one sub-frame. Therefore, proactive protocol is best choice for broadcast and multicast communication.

4.3.3 Case II : Requests following normal distribution

Fig. 4.18 shows the graph of normally generated D2D requests per timeslot and Fig. 4.19 shows the graph of probability density function (PDF) of normally generated requests per timeslot. Assume that N is the total number of UE-E(s) which generate the D2D request and M is the number of requests generated per times-

lot which follows the normal distribution. The PDF of normally generated D2D requests is calculated as in equation 4.10 [29]

$$PDF = \frac{1}{\sigma\sqrt{2\pi}} \exp^{-} \frac{(M-\mu)^2}{2\sigma^2} \tag{4.10}$$

where μ is the mean value of the D2D requests generated by UE-Es and σ is the standard deviation of the normal Gaussian distribution. The value of μ is 2.14 and value of σ is 3.8. Protocol overhead for proactive and reactive protocol for

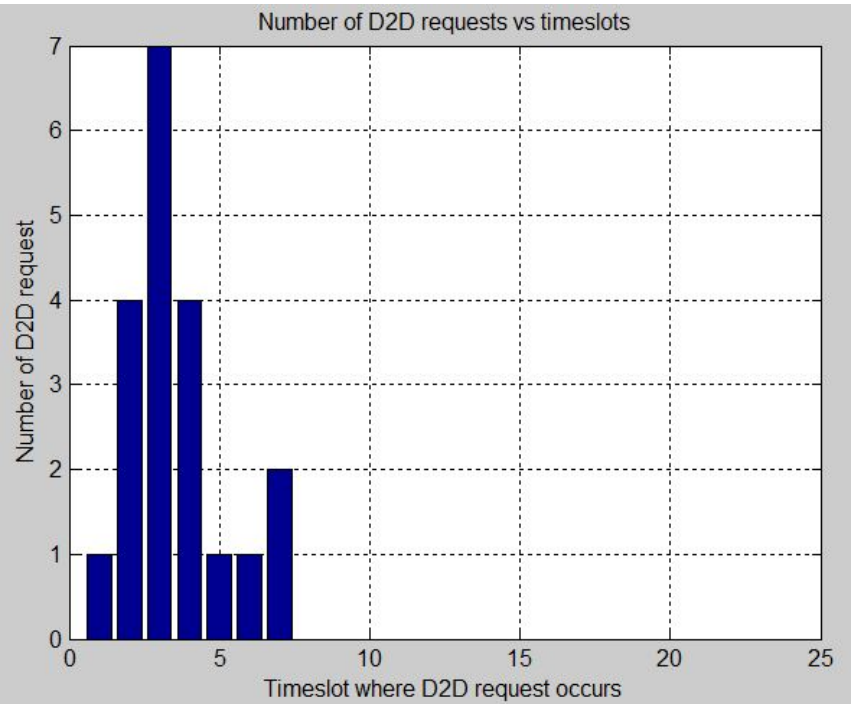


Figure 4.18: Normally distributed D2D requests.

normally distributed D2D requests is calculated as follows:

$$CO_p = \frac{2 \times (T - T') + T' \times (2 + 14 \times M)}{T} \tag{4.11}$$

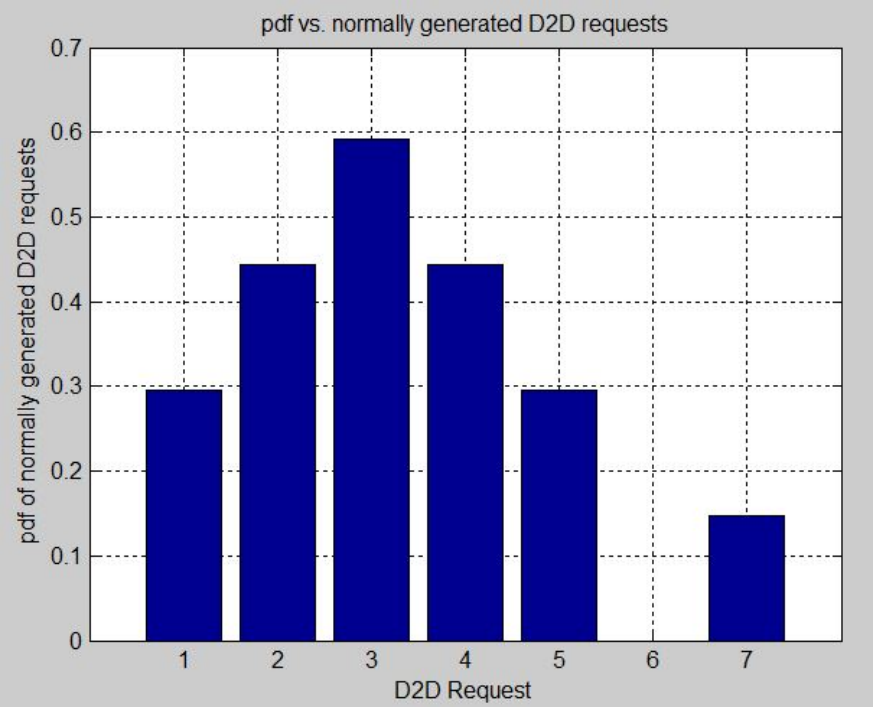


Figure 4.19: PDF of normally generated D2D requests.

$$CO_r = \frac{(T' \times 15 \times M)}{T} \tag{4.12}$$

where CO_r denotes control overhead of reactive protocol and CO_p denotes control overhead for proactive protocol.

Result of case II

Tab. 4.2 explains the necessary network parameters to calculate the control overhead for both proactive and reactive protocols. Fig. 4.20 shows the protocol overhead vs. normally distributed D2D request. As shown in the graph, with higher number of the D2D request at each timeslot, control overhead of reactive increases in comparison with proactive protocol. Therefore, proactive protocol is preferred when D2D requests are normally distributed.

Table 4.2: Network parameters configuration to calculate control overhead for case II

Parameters	*Symbols*	*Values*
Total number of UE-Es.	N	10
Total timeslots.	T	20
Timeslots where D2D request occurs	T'	T
D2D request at each timeslots	M	[0 to N]

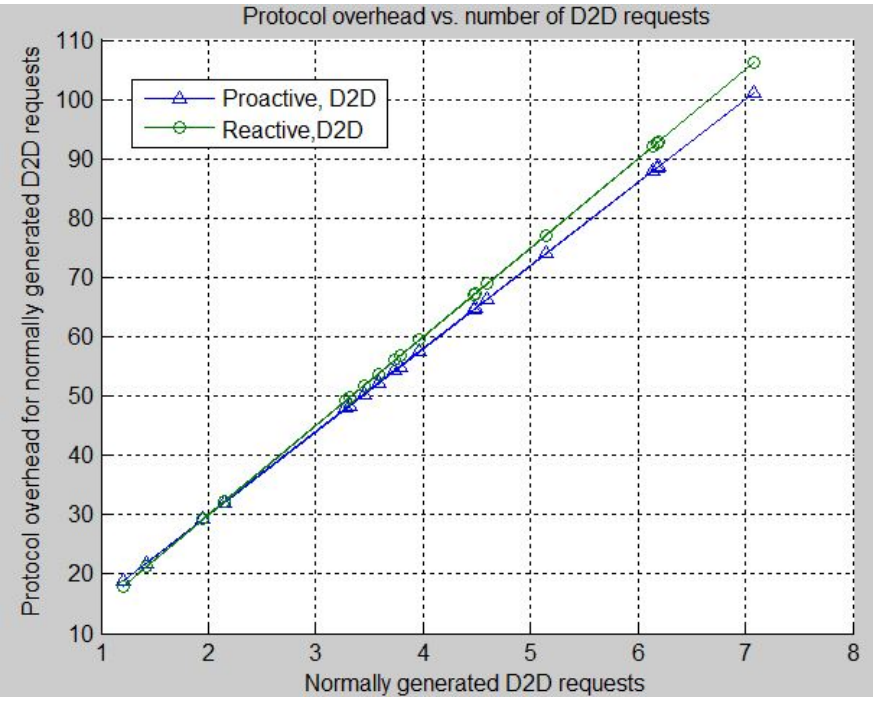


Figure 4.20: Control overhead vs. normally distributed D2D request.

4.3.4 Case III : Random occurrence of D2D requests

Fig. 4.21 shows random occurrence of D2D request at each timeslot. In this case, the number of D2D request per timeslot is not fixed. The protocol overhead for both proactive and reactive protocol are calculated as follows:

$$CO_p = \frac{T' \times (2 + (14 \times M)) + (2 \times (T - T'))}{T} \tag{4.13}$$

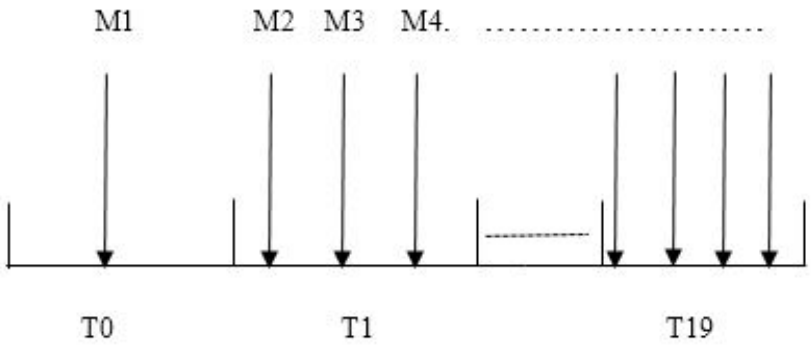


Figure 4.21: Random distribution of UE-Es.

$$CO_r = \frac{(T' \times 15 \times M)}{T} \tag{4.14}$$

Result of case III

Network parameters to calculate the protocol overhead for case III is listed in Tab. 4.3. We can see in Fig. 4.22, proactive protocol has relatively more control overhead when there is no D2D request. Reactive protocol has less overhead till number of D2D requests are 2. Both protocol has same overhead when D2D requests are from 2 to 4. Proactive protocol has less protocol overhead in comparison to reactive protocol as number of requests increase. In Fig. 4.23, when target distance increases number of UE-Es also increase. More UE-Es mean there is more possibility to have D2D requests. For more D2D requests proactive performs better because it has less overhead in comparison to reactive protocol. Therefore, If more UE-E(s) are participating in D2D communication proactive protocol is selected otherwise reactive is preferable.

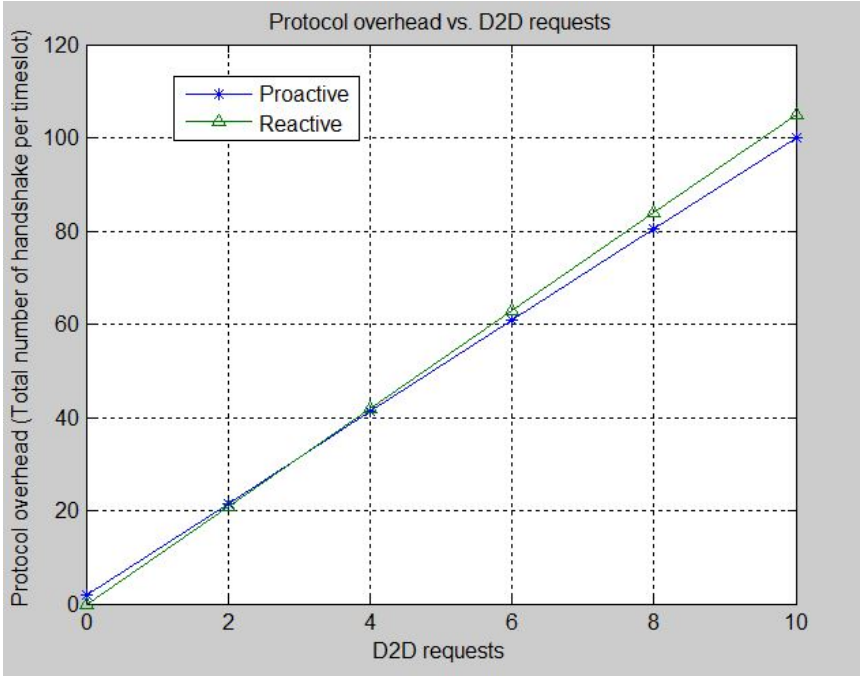


Figure 4.22: Protocol overhead vs. D2D requests

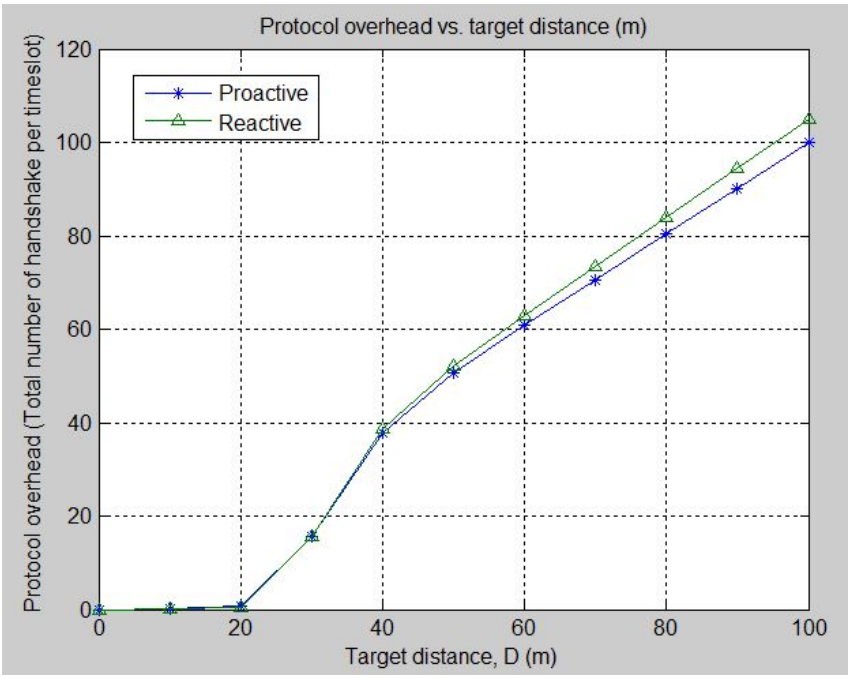


Figure 4.23: Protocol overhead vs. target distance

Table 4.3: Network parameters configuration to calculate control overhead for case III

Parameters	*Symbols*	*Values*
Total number of UE-Es.	N	10
Total timeslots.	T	20
Timeslots where D2D request occurs	T'	T
D2D request at each timeslots	M	[0 to N]
Targeted distance	d	0 to 100 meter

4.4 Chapter Summary

This chapter has presented the implementation of the proposed protocols using SDL. The SDL diagrams from UE-E's, UE-R's, BS's and AS's prospective has represented in this chapter. We verified the proposed protocols successfully using SPIN model checker without errors. To compare the two proposed protocols in terms of protocol overhead, numerical calculation has performed in MATLAB simulation. For selected scenarios, the UE-Es are situated outside coverage area and are distributed randomly according to the Poisson point process. We used binomial distribution function to calculate the probability function for at least k UE-E(s) make D2D pair with UE-R. Three different cases for D2D requests as same number of D2D requests, requests follows normal distribution and random occurrence of D2D requests has considered to calculate the protocol overhead. According to the result, reactive protocol has relatively more protocol overhead in comparison to proactive protocol when there is many D2D requests. However, proactive protocol has high overhead for less number of requests than reactive protocol. Therefore, proactive protocol is preferred in scenarios where there is relatively high number of D2D requests whereas reactive is preferred for less number of D2D requests.

Chapter 5

Security Enhancement of the Proposed Protocols

In this chapter the security challenges and possible threats related to D2D communication are discussed. In addition, proposed security enhancement protocol for mutual authentication and establishment of common secret key are explained. The proposed protocol is analyzed and validated using SPIN model checker.

5.1 Security Challenges and Threats

There are many reasons behind weak security system in D2D communication for selected scenario. In such scenario, there is no network infrastructure to monitor the suspicious activities performed by UEs [4]. D2D communication is based upon wireless communication. Wireless communication is itself vulnerable to many security threats such as man in the middle attack, modification of data, replay attack, identity spoofing, denial of service attack, jamming [3]. Hence, D2D communication inherits all the security threats of wireless communication. Security is one of the important and major concerns for the D2D communications which should be addressed before implementing it. In proposed security enhancement protocol, we have assumed that communicating UEs are not compromised and it only prevents the intruder to intercept the messages exchanged between UEs.

A D2D communication is said to be secure if it preserves the CIAAA of information transmitted over D2D channel. Confidentiality will preserve the privacy of information and only authorized user can have access to the information. Integrity will make sure that the information is not modified during transmission by any user. Authentication service allows only authenticated user can access the information. Similarly, availability allows legitimate users to access the information from anywhere at any time [5]. If any one of above mentioned security conditions break down then intruder can easily take over the D2D communication link and do whatever he/she wants to do with the messages exchanged over it. Some of the security threats that might happen in D2D communication [3] are described as follows:

- Man in the middle (MIM) attack: The D2D link is considered to be insecure mode of communication. Therefore, if proper security is not applied before transmission, an intruder can intercept the messages transmitted over D2D link and modify as per its requirement and transmit it to the destination UE. An intruder makes a separate connection with both the UEs. Both UEs do not have any idea about attack and continue communication as if messages are originated from legitimate user.

- Replay attack: In replay attack, an intruder record the messages and retransmit or repeat the messages after certain time interval in the same network or in different networks. The message is legitimate and it is quite difficult to identify that the messages is not from the legitimate user.

- Identity spoofing: In identity spoofing attack, an intruder spoofs the identity of legitimate UEs or use any identity which does not exist in the given network. Spoofed UEs start D2D communication and use the ProSe provided by D2D communication even though it is not eligible to use which leads to misuse of resources.

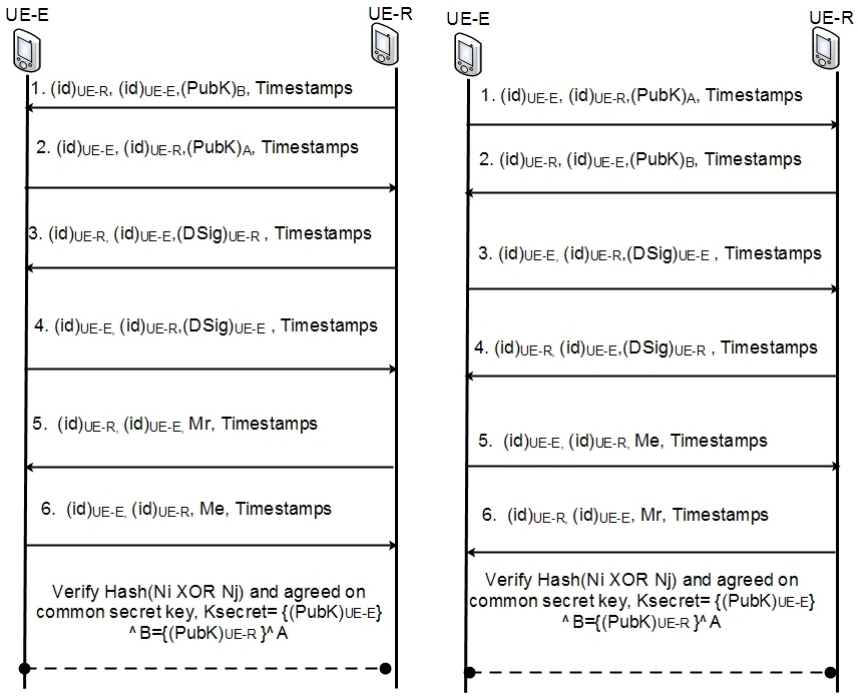
- Denial of service (DoS): In DoS attack, one or many malicious UE-Es continuously send D2D request to UE-R. Due to the limited capacity of UE-R it can not proceed all the requests send by UE-Es which causes DoS attack. In addition, the heavy traffic in D2D channel consumes large amount of

resources. Since the resources in D2D communication is limited, this will cause actual UE-E users unable to access the services offered by UE-R.

5.2 Security Protocol Design

In this Master's thesis, security enhancement protocol for mutual authentication of UEs and establishment of common secret key based upon Diffi-Hellman key exchanged algorithm has been proposed. The proposed protocol is applicable for both proactive and reactive protocols as shwon in Fig. 5.1. In case of reactive protocol, UE-R initiates the authentication process as shown in Fig. 5.1a where as in proactive protocol, UE-E initiates the authentication process as shown in Fig. 5.1b. According to Diffi-Hellamn key exchanged algorithm [5], two UEs established a common secret key which can be used as a secret key to encrypt/decrypt the messages. Communicating UEs themselves are responsible for establishment of secret key because there is not available of any key distribution infrastructure [25].

First of all, UE-E and UE-R generates the secret number A and B respectively and compute public key (PubK). PubK computed by UE-R is $(PubK)_{UE-R} = g^B mod P$ whereas public key computed by UE-E is $(PubK)_{UE-E} = g^A mod P$, where g is common generator, $B \in (1, 2, 3, ...P - 1)$, $A \in (1, 2, 3, ...P - 1)$ and P is large prime number. P and g are known to all UEs in networks. UE-R and UE-E generates the nonce N_j and N_i respectively. UE-R generates the hash value of N_j and encrypt it by secret number B and attach with nonce N_j. The resulting value is called digital signature (DSig) of UE-R which is given by, $(DSig)_{UE-R} = \{Encrypt[Hash(N_j), B], N_j\}$. Similarly, UE-E generates the hash value of N_i which is encrypted by secret number A and attach with nonce N_i. The resulting value is called digital signature of UE-E and is given by, $(DSig)_{UE-E} = \{Encrypt[Hash(N_i), A], N_i\}$. UE-R extract the N_i from digital signature and compute notification message as $M_r = Encrypt\{Hash(N_i \oplus N_j), (PubK)_{UE-E}\}$. Similarly, UE-E extract the N_j from digital signature and compute notification message as $M_e = Encrypt\{Hash(N_j \oplus N_i), (PubK)_{UE-R}\}$. The number of steps require for mutual authentication as well as to agree on common secret key are described as follows:



(a) (b)

Figure 5.1: (a) Security enhancement protocol for reactive and (b) Security enhancement protocol for proactive.

- Step 1: Once UE-R receive *discovery request* from UE-E, UE-R send $(PubK)_{UE-R}$ along with $(id)_{UE-R}$, $(id)_{UE-E}$ and $Timestamps$ at which message is generated,
- Step 2: UE-E send $(PubK)_{UE-E}$ along with $(id)_{UE-E}$, $(id)_{UE-R}$ and $Timestamps$ at which message is generated,
- Step 3: UE-R calculate $(DSig)_{UE-R}$ and send along with $Timestamps$ at which signature is generated to UE-E,
- Step 4: UE-E calculate $(DSig)_{UE-E}$ and send along with $Timestamps$ at which signature is generated to UE-E.
- Step 5:UE-R send M_r,
- Step 6: UE-E send M_e.

Both UE-E and UE-R decrypt M_r and M_e with their private key and verify the hash($N_i \oplus N_j$). After verification, both UEs agree on establishment of secret key, K_{secret} called common secret key which is used to encrypt/decrypt the rest of the messages. K_{secret} is computed as $K_{secret} = ((PubK)_{UE-E})^B = ((PubK)_{UE-R})^A$

5.3 Security Analysis of the Enhanced Protocol

To preserve CIAAA of an information, it is necessary to encrypt and digitally sign the messages with their secret key, which only authorized or authenticated UEs can decrypt and verify [5]. Our aim is to protect the messages exchanged between UEs from intruder. For this purpose, we designed a protocol with the security enhancement. The communication channel between UEs are public, so it is possible to intercept the messages by intruder. Two UEs must be ensured that they are communicating with legitimate UEs. This can be achieved by the process of mutual authentication. Generally, the security mechanism between BS and UE is based upon the standard existing security mechanism offered by LTE-A [3]. However, due to the lack of centralized security infrastructure for D2D communication, security becomes quite difficult. During this Master's thesis, our focus is to authenticate two UEs and establish a common secret key which is only known to participating UEs.

The proposed security protocol is divided into two phases, mutual authentication phase and notification phase. During mutual authentication phase, digital signature is used to authenticate each other whereas in notification phase two UEs notify one another that they have authenticated each other. In this protocol, each messages are send along with $Timestamps$. $Timestamps$ is used to prevent the Replay attack. Since there is possibility to record the messages and send it in another time period. By the use of $Timestamps$, receiver checks the sender's $Timestamps$ and compare it with its own $Timestamps$ at which message received. If the difference is intolerance, message will be discarded. In this way $Timestamps$ can prevent the Replay attack. Similarly, both the UEs generates the nonce so that the old information can not be used in Replay attack. nonce is the random number that is used only once in the cryptography communication.

Digital signature is used to verify the identity of sender as well as for integrity

of the data [5]. Anyone in the network can verify the digitally signed signature because all users in the network know the public key of sender but only sender can digitally sign the message because only sender has access to the private key. Therefore, verifying digital signature ensure that the sender UE is legitimate. In the proposed security protocol, hash value of nonce is computed which is then encrypted with UE's secret number which is called certificate. Certificate along with nonce is called digitally signed data. During the verification of signature, receiving UE extracts the nonce and signature. Receiver then compute the hash value of nonce as well as decrypt the signature with sender's public key and recover the hash value of nonce. Now receiver compare the computed hash value and recovered hash value of data. If both hash value match then receiver verifies that the sender is actual and legitimate and data are not tampered on its way. Hence, it also preserves the integrity of messages.

After mutual authentication, both UEs should notify each other that they authenticate each other. For the notification process, UE-R and UE-E compute the notification message M_r and M_e respectively. UE-E and UE-R decrypt the M_r and M_e respectively and extract hash($N_i \oplus N_j$). Both UEs compare received hash value with their own hash value. If computed hash value and received hash value are equal then they agree to establish a common secret key which can be used as secret key for message encryption/decryption process. The hash value of exclusive OR (XOR) of both nonce are encrypted with each others public key. Therefore, to decrypt M_r and M_e UE-E and UE-R should know their respective private key. So it is almost impossible for any intruder to modify the M_e and M_r on its way. In addition, the secret key is not exchanged during communication process. Onle g, P, and theirs public keys are knows to intruder. Even for super speed modern computers it is difficult to find secret value A and B with given g, P, $(PubK)_{UE-R}$ and $(PubK)_{UE-E}$. Such problem is called discrete logarithm problem [30]. Therefore, intruder won't able to intercept the secret key that UEs has agreed on.

5.4 Proposed Protocols with Security Enhancement

Fig. 5.2 and Fig. 5.3 show the proposed neighbor and service discovery protocols with security enhancement.

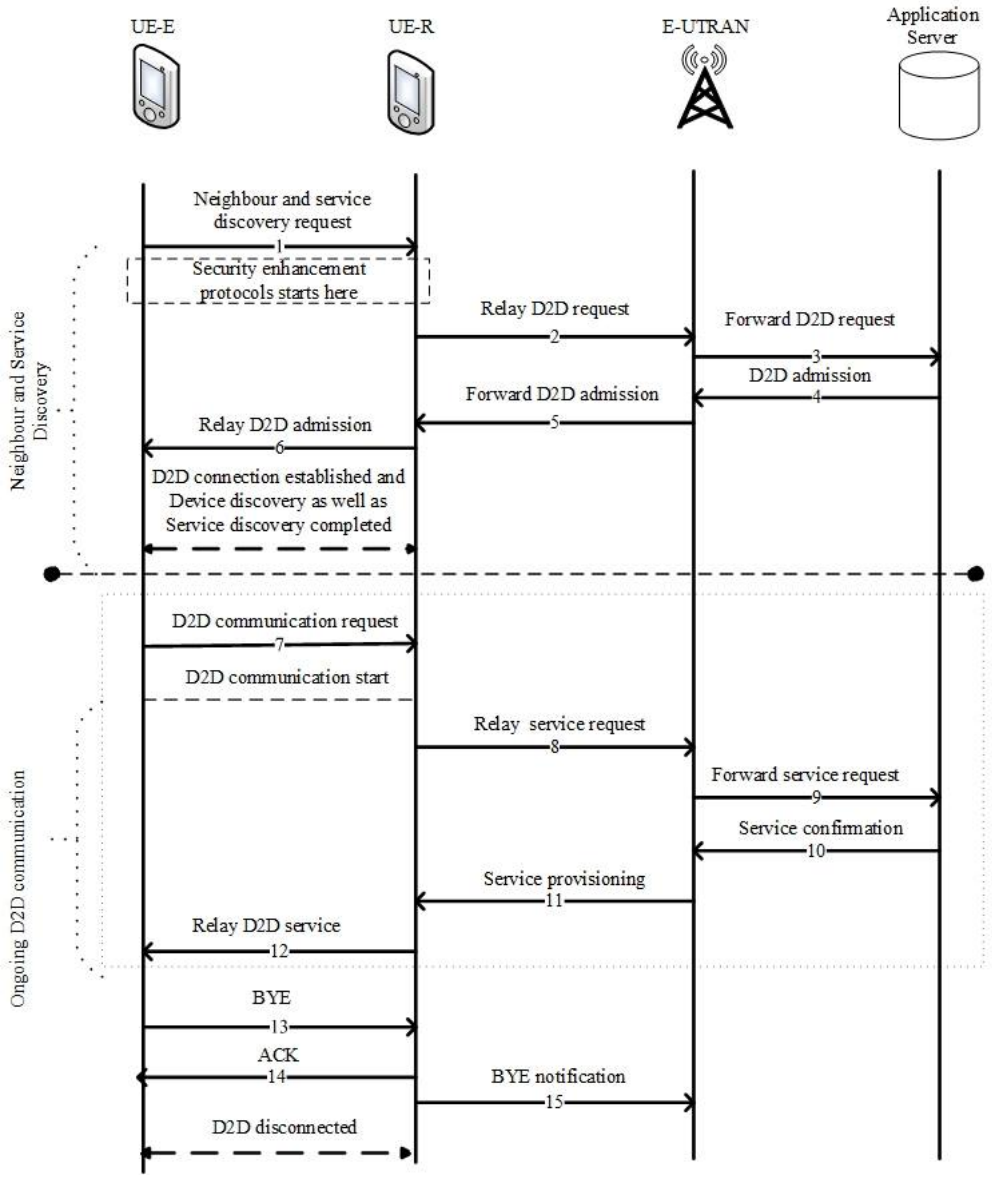


Figure 5.2: Reactive protocol with security enhancement.

The security enhancement protocol is added in proposed discovery protocols design. For reactive protocol, security enhancement protocol is initiated by UE-R after it receives *Neighbor and discovery request* from UE-E. UE-R does not relay the request send by UE-E to BS until it authenticate UE-E as shown in Fig. 5.2. For proactive protocol, UE-E initiates the security enhancement protocol after it received *Multicast D2D service invitation* from UE-R as in Fig. 5.3.

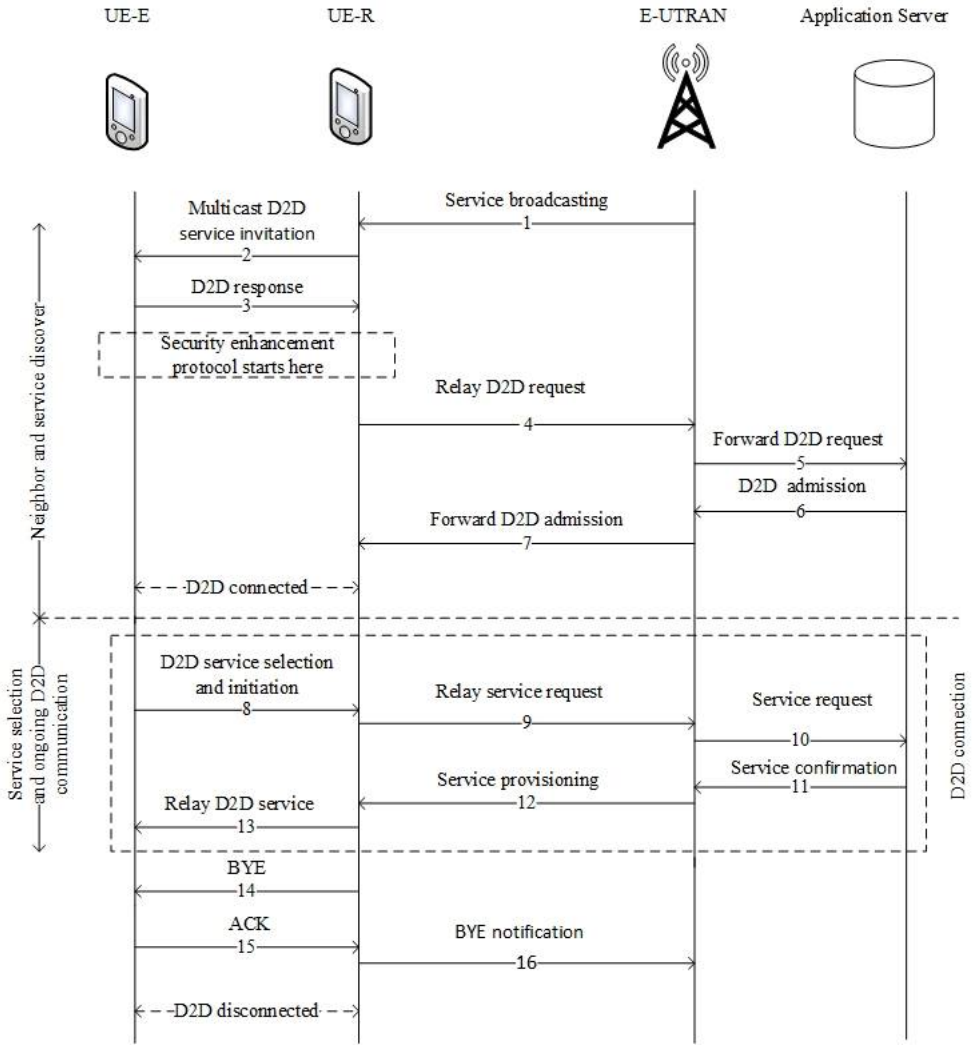
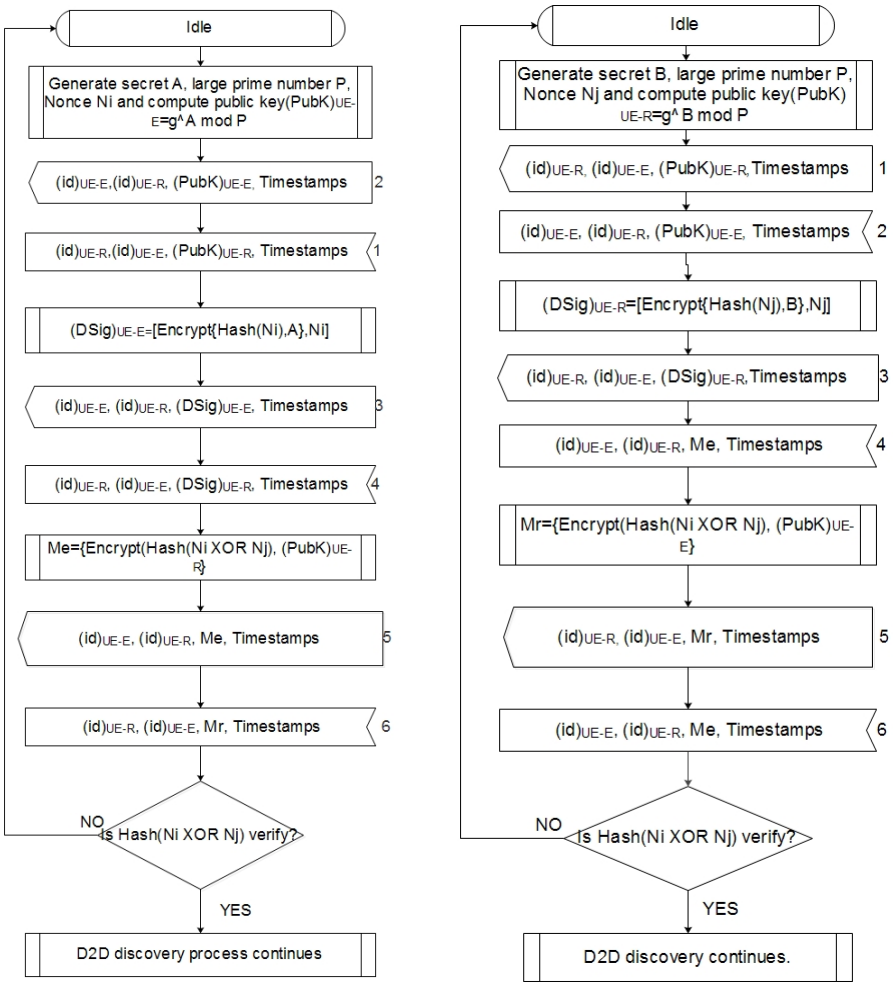


Figure 5.3: Proactive protocol with security enhancement.

5.5 Protocol Implementation using SDL

The SDL implementation for the UE-R and UE-E according to the security enhancement protocol are shown in Fig. 5.4a and Fig. 5.4b respectively.

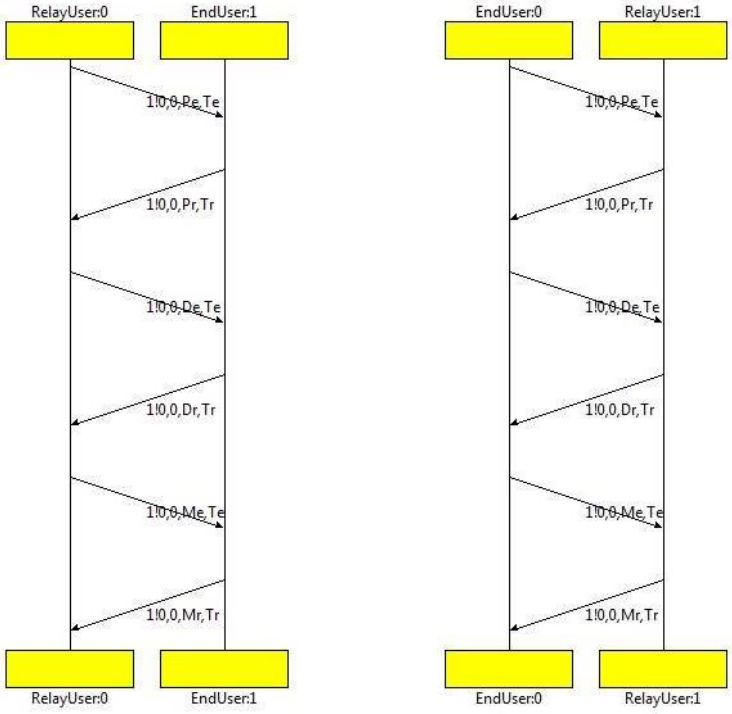


(a) (b)

Figure 5.4: SDL diagram from (a) UE-E's prospective and (b) UE-R's prospective.

5.6 Protocol Validation using SPIN

The validation output for the proposed security enhancement protocol is shown in Fig. 5.5a and Fig. 5.5b. As shown in Fig. 5.5a, in reactive protocol, UE-R initiate the authentication process by sending its public key, P_r to UE-E. UE-E responds with sending its public key, P_e to UE-R. After verification of digital signature D_r and D_e by UE-E and UE-R respectivley they verify hash($N_i \oplus N_j$) contains in messages M_r and M_e. T_r and T_e are the timestamps used by UE-E and UE-R at which messages are generated to prevent the replay attack. Security enhancement protocol works in the same manner for proactive protocol except UE-E initiates the authentication process after receiving service broadcast message from UE-R as in Fig. 5.5b.



(a) (b)

Figure 5.5: SPIN verification output for security enhancement protocol (a) Reactive protocol and (b) Proactive protocol.

SPIN verification output

The verification output of security enhancement protocol for reactive and proactive protocols are shown in Fig. 5.6 and Fig. 5.7 respectively. As it can be seen from output that both protocol verifies without errors and reached to the depth 18.

```
State-vector 28 byte, depth reached 18, errors: 0
      19 states, stored
       0 states, matched
      19 transitions (= stored+matched)
       0 atomic steps
hash conflicts:         0 (resolved)

Stats on memory usage (in Megabytes):
   0.001   equivalent memory usage for states (stored*(State-vector + overhead))
   0.291   actual memory usage for states
  64.000   memory used for hash table (-w24)
   0.343   memory used for DFS stack (-m10000)
  64.539   total actual memory usage
```

Figure 5.6: SPIN verification output of security enhancement protocol for reactive protocol.

```
State-vector 28 byte, depth reached 18, errors: 0
      19 states, stored
       0 states, matched
      19 transitions (= stored+matched)
       0 atomic steps
hash conflicts:         0 (resolved)

Stats on memory usage (in Megabytes):
   0.001   equivalent memory usage for states (stored*(State-vector + overhead))
   0.291   actual memory usage for states
  64.000   memory used for hash table (-w24)
   0.343   memory used for DFS stack (-m10000)
  64.539   total actual memory usage
```

Figure 5.7: SPIN verification output of security enhancement protocol for proactive protocol.

5.7 Chapter Summary

This chapter has proposed security enhancement protocol for neighbor and service discovery protocols, reactive and proactive. This chapter has explained the security challenges and the possible threats for the selected scenarios of D2D communication. The proposed security enhancement protocol is based on Diffi-Hellman key exchanged algorithm. Digital signature is used to mutually authenticate two communicating UEs. Notification messages is exchanged to notify each other about the confirmation of verification. After verification process, UE-E and UE-R agreed on common secret key, which can be used for encryption/decryption of the messages exchanged between them. Security enhancement protocol is initiated in proposed reactive protocol after UE-R receives discovery message from UE-E. On the other hand, in proposed proactive protocol, security enhancement protocol is initiated by UE-E after receiving ”Multicast D2D service invitation” message from UE-R. Security enhancement protocol is implemented and validated by using SDL and SPIN model checker respectively. The proposed security protocol validated successfully without errors.

Chapter 6

Conclusions and Future Work

This chapter summarize thesis work, contribution based on our findings and suggestion for future work.

6.1 Summary

This thesis presents work related to D2D communication. The first part of the project was a summarization of the general concepts of D2D communication and its enabling technologies. By studying 3GPP technical reports and its suggested scenarios for D2D communication, one scenario is selected as primary scenario. In the scenario, UE-R is located inside and UE-E is located outside of coverage area. Based on this scenario, reactive and proactive protocols are proposed. Furthermore, the implementations of the mentioned protocols design using SDL. The proposed protocols are validated using SPIN model checker. The obtained simulation and verification results were represented.
Furthermore, this Master's thesis has given discussion about the possible D2D security challenges and threats, proposed security protocol for mutual authentication and establishment of common secret key, protocol analysis and validation of proposed protocol.

6.2 Contributions

This Master's thesis has contributed in following areas:

- The two neighbor and service discovery protocols have been proposed for scenario 1B as suggested by 3GPP for D2D communication. Both protocols give an overview of how UEs discover each other when UE-E(s) is located outside network coverage area and UE-R is located inside coverage area with out getting support from BS.
- The proposed protocols with and without security enhancement have been implemented and verified.
- The two proposed protocols have been compared in terms of protocol overhead which was calculated in MATLAB simulation environment. This thesis suggests which protocol is suitable for D2D communication for selected scenario based on overhead calculation. For the calculation, different cases of D2D requests have been considered.
- The security enhancement protocol based on Diffi-Hellman algorithm has been proposed in order to mutually authenticate UE-E and UE-R as well as common secret key has been established to encrypt/decrypt the handshake messages.

6.3 Future Work

Research on D2D communication has been a hot topic taking the attention of many scientific researchers in mobile technology. We presented two protocols design for D2D communication. However, future works are needed to improve the performance of our proposed protocols. For future work, it is suggested:

- Using different use case scenario to improve the usability and efficient of our protocols in real world environment.
- To proposed protocol for D2D communication between multiple UE-Rs and one UE-E.

- Improve the security of proposed protocols using a lightweight encryption/decryption scheme.

Bibliography

[1] 3GPP, "Study on architecture enhancements to support," Tech. Rep., Jun 2013. [Online]. Available: http://www.3gpp.org/DynaReport/23703.htm

[2] ——, "Study on LTE device to device proximity services," 3GPP A global initiative, 650 Route des Lucioles - Sophia Antipolis Valbonne - FRANCE, Tech. Rep., Mar.

[3] M. Alam, D. Yang, J. Rodriguez, and R. Abd-Alhameed, "Secure device-to-device communication in lte-a," *Communications Magazine, IEEE*, vol. 52, no. 4, pp. 66–73, April 2014.

[4] S. Ramasubramanian, S. Chung, L. Ding, and S. Ryu, "Secure and smart media sharing based on direct communications among mobile devices underlying in lte-a cellular network."

[5] M. Stamp, *Information security: principles and practice*. John Wiley & Sons, 2011.

[6] Z.-J. Yang, J.-C. Huang, C.-T. Chou, H.-Y. Hsieh, C.-W. Hsu, P.-C. Yeh, and C.-C. Hsu, "Peer discovery for device-to-device (d2d) communication in lte-a networks," in *Globecom Workshops (GC Wkshps), 2013 IEEE*, Dec 2013, pp. 665–670.

[7] S. Alamouti and A. Sharafat, "Resource allocation for energy-efficient device-to-device communication in 4g networks," in *Telecommunications (IST), 2014 7th International Symposium on*, Sept 2014, pp. 1058–1063.

[8] Y. Zhao, B. Pelletier, P. Marinier, and D. Pani, "D2d neighbor discovery interference management for lte systems," in *Globecom Workshops (GC Wkshps), 2013 IEEE*. IEEE, 2013, pp. 550–554.

[9] D. Wu, L. Zhou, Y. Cai, R. Hu, and Y. Qian, "The role of mobility for d2d communications in lte-advanced networks: energy vs. bandwidth efficiency," *Wireless Communications, IEEE*, vol. 21, no. 2, pp. 66–71, April 2014.

[10] 3GPP, "Proximity-based services (prose);stage 2(release 12)," 3GPP, Tech. Rep., feb 2014. [Online]. Available: http://www.3gpp.org/dynareport/23.303.htm

[11] A. Thanos, S. Shalmashi, and G. Miao, "Network-assisted discovery for device-to-device communications," in *Globecom Workshops (GC Wkshps), 2013 IEEE*, Dec 2013, pp. 660–664.

[12] 3GPP, "Proximity-services (prose) user equipment (ue) to prose function protocol aspects; stage 3(release 12)," 3GPP, Tech. Rep., Jan 2015. [Online]. Available: http://www.3gpp.org/dynareport/24.334.htm

[13] F. Ahishakiye, "Neighbor discovery and resource allocation for device-to-device communication," Master's thesis, Universitetet i Agder; University of Agder, 2014.

[14] G. J. Holzmann, *The SPIN model checker: Primer and reference manual*. Addison-Wesley Reading, 2004, vol. 1003.

[15] G. Holzmann, "The model checker spin," *Software Engineering, IEEE Transactions on*, vol. 23, no. 5, pp. 279–295, May 1997.

[16] E. visualization solutions, "Specification and description language." [Online]. Available: https://www.edrawsoft.com/SDL-Diagrams.php

[17] D. Tsolkas, E. Liotou, N. Passas, and L. Merakos, *LTE-A Access, Core, and Protocol Architecture for D2D Communication*. Springer Cham Heidelberg New York Dordrecht London, 2014.

[18] M. Corici, D. Vingarzan, T. Magedanz, and T. Magedanz, "3gpp evolved packet core - the mass wireless broadband all-ip architecture," in *Telecommunications: The Infrastructure for the 21st Century (WTC), 2010*, Sept 2010, pp. 1–6.

[19] 3GPP, "Long term evolution," 2006. [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte

[20] ——, "Long term evolution-advanced," jun 2013. [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced

[21] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, and N. Brahmi, "Device-to-device communications for national security and public safety," *Access, IEEE*, vol. 2, pp. 1510–1520, 2014.

[22] L. Goratti, G. Steri, K. Gomez, and G. Baldini, "Connectivity and security in a d2d communication protocol for public safety applications," in *Wireless Communications Systems (ISWCS), 2014 11th International Symposium on*, Aug 2014, pp. 548–552.

[23] F. Ahishakiye and F. Li, "Service discovery protocols in d2d-enabled cellular networks: Reactive versus proactive," in *Globecom Workshops (GC Wkshps), 2014*, Dec 2014, pp. 833–838.

[24] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 4, pp. 1801–1819, Fourthquarter 2014.

[25] W. Shen, W. Hong, X. Cao, B. Yin, D. Shila, and Y. Cheng, "Secure key establishment for device-to-device communications," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, Dec 2014, pp. 336–340.

[26] 3GPP, "Feasibility study for Proximity Services (ProSe) (Release 12)," Tech. Rep., Jun 2013. [Online]. Available: http://www.3gpp.org/DynaReport/22803.htm

[27] Q. Yanhuai, F. Jianan, and S. Zhang, "Nearest neighbor nodes and connectivity of wireless sensor networks with poisson point process," in *Control Conference (CCC), 2010 29th Chinese*, July 2010, pp. 4776–4780.

[28] J. W. Harris and H. Stöcker, *Handbook of mathematics and computational science*. Springer Science & Business Media, 1998.

[29] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[30] A. Abdouli, J. Baek, and C. Y. Yeun, "Survey on computationally hard problems and their applications to cryptography," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, Dec 2011, pp. 46–52.

Appendices

Appendix A

PROMELA code

(i) PROMELA code for reactive protocol

```
    mtype = { discovery_req, ack, d2d_adm, service_req, got_service, BYE}
byte idE;
byte idR;
byte idB;
byte idA;
byte Ecode;
chan BR = [1] of { mtype};
chan ER = [1] of { mtype};
chan BA = [1] of { mtype};
int count=2;
bool tmpEnd, tmpBS, tmpRelay;
int To=5;


active proctype EndUser()
{

T0:     ER!discovery_req;

    if
    ::ER?d2d_adm

    ::tmpEnd==To -> goto T0
    fi;



T5:     ER!service_req;

    if
    ::ER?got_service
```

```
    :: tmpEnd==To ->
            if
            ::(count!=0);
            do
            ::count=count-1->goto T5
            ::else ->break
            od
            ::(count==0) ->skip
            fi
    fi;


T7: ER!BYE;

    if
    ::ER?ack->skip
    ::tmpEnd==To ->skip
    fi
    }

active proctype RelayUser()
{
T0: ER?discovery_req;
T2: BR!discovery_req;
    if
    ::BR?d2d_adm
    :: tmpRelay==To->
            if
            ::(count!=0);
            do
            ::count=count-1->goto T2
            ::else->break
            od
            ::(count==0)-> skip
            fi
    fi;
    ER!d2d_adm;
T8: ER?service_req;
T10:    BR!service_req;
    if
    ::BR?got_service
    ::tmpRelay==To ->
    if
    ::(count!=0);
    do
    ::count=count-1->goto T10
    ::else->break
    od
    ::(count==0) -> skip
```

```
    fi
    fi;
ER!got_service;
T16:    ER?BYE;
T18:    ER!ack;
T20:    BR!BYE
}

active proctype BaseStation()
{
T1: BR?discovery_req;
T3: BA!discovery_req;
    if
    ::BA?d2d_adm
    ::(tmpBS==To)->
        if
        ::(count!=0);
        do
        ::count=count-1->goto T3
        ::else ->break
        od
        ::(count==0)->skip
        fi
    fi;
T8:   BR!d2d_adm;
T10:      BR?service_req;
T12:      BA!service_req
      if
    ::BA?got_service
    ::tmpBS==To->
            if
            ::(count!=0);
            do
            ::count=count-1->goto T12
            ::else ->break
            od
            ::(count==0)->skip
            fi;
    fi;
    BR!got_service;
    BR?BYE
     }

active proctype AppServer()
{
BA?discovery_req;
BA!d2d_adm;
BA?service_req;
BA!got_service;
```

```
}
```

(ii) PROMELA code for proactive code

```
mtype = { broad, d2d_req,d2d_inv, multc_s, d2d_resp, ack, d2d_adm, serv_req,

chan BR = [1] of { mtype };
chan BA = [1] of { mtype };
chan ER = [1] of { mtype };
byte count=2;
byte count_br=2;
byte To=5;


proctype BS()
{
bool tmpBS;

S1: BR!broad;
    if
    ::BR?d2d_req;
S2: BA!d2d_req;

        if
        ::BA?d2d_adm;
S3:       BR!d2d_adm;
            if
            ::BR?serv_req;
S4:         BA!serv_req;
                if
                ::BA?serv_confirm;
                  BR!serv_confirm;
                  BR?BYE
                ::tmpBS==To->
                if
                ::(count!=0)->
                    do
                    ::count=count-1 -> goto S4
                    ::else->break
                    od
                ::(count==0)-> printf("idle")
                fi
                fi



            ::tmpBS==To-> goto S3
        fi
```

```
            ::tmpBS==To->goto S2
            fi
        ::tmpBS==To->
            if
                    ::(count_br!=0)->
                        do
                        ::count_br=count_br-1 -> goto S1
                        ::else->break
                        od
                    ::(count==0)-> printf("idle")
            fi


        fi

    }

    proctype AppServer()
    {
    bool tmpAppS;

        if
        ::BA?d2d_req;
        BA!d2d_adm
        ::tmpAppS==To->printf("Idle")
        fi

         if
        ::BA?serv_req;
        BA!serv_confirm
        ::tmpAppS==To->printf("Idle")
        fi



    }
    proctype EndUser()
    {
    bool tmpEnd;

        ER?d2d_inv;
        ER!d2d_resp;

        ER?multc_s;

    S3: ER!serv_req;
                if
                ::ER?serv_confirm;
```

```
                ER?BYE;
                    ER!ack;
                    printf("Idle");

                ::tmpEnd==To->
                    if
                    ::(count!=0);
                        do
                        ::count=count-1->goto S3
                        ::else->break
                        od
                    ::(count==0)->printf("Idle")
                    fi
                fi

}

proctype RelayUser ()
{
bool tmpRelay;

    BR?broad;
S1:     ER!d2d_inv;
        if
        ::ER?d2d_resp;

S2:     BR!d2d_req;
            if
            ::BR?d2d_adm;


S3:         ER!multc_s;
                if
                ::ER?serv_req;

S4:             BR!serv_req;
                    if
                    ::BR?serv_confirm;
                    ER!serv_confirm;

                    ER!BYE;

                        if
                        ::ER?ack;
                        BR!BYE;
                        ::tmpRelay==To;
                        BR!BYE;
                        fi
```

```
                        ::tmpRelay==To-> goto S4
                        fi


                    ::tmpRelay==To-> goto S3
                    fi

                ::tmpRelay==To;
                    if
                        ::(count!=0);
                        do
                        ::count=count-1 -> goto S2
                        ::else->break
                        od
                        ::(count==0)->printf("Idle")
                    fi

                fi
            ::tmpRelay==To;
                if
                ::(count_br!=0);
                    do
                    ::count=count-1 -> goto S1
                    ::else->break
                    od
                ::(count==0)->printf("Idle");
                fi
            fi

}


init {run EndUser(); run RelayUser (); run BS (); run AppServer ();}
```

(iii) PROMELA code for security enhancement protocol

```
mtype={Pe,Pr,Te,Tr,De,Dr,Me,Mr};
chan ER= [1] of {byte,byte,mtype,mtype};
    byte idE;
    byte idR;
active proctype EndUser()
{
    ER!idE,idR,Pe,Te;
    ER?idR,idE,Pr,Tr;
    ER!idE,idR,De,Te;
    ER?idR,idE,Dr,Tr;
```

```
        ER!idE,idR,Me,Te;
        ER?idR,idE,Mr,Tr;
        if
        ::(Me==Mr)->printf("UE-E authenticate UE-R");
        ::else->skip
        fi

    }

    active proctype RelayUser()
    {
    S2: ER?idE,idR,Pe,Te;
        ER!idR,idE,Pr,Tr;
        ER?idE,idR,De,Te;
        ER!idR,idE,Dr,Tr;
        ER?idE,idR,Me,Te;
        ER!idR,idE,Mr,Tr;
        if
        ::(Me==Mr)->printf("UE-R authneticate UE-E")
        ::else->skip
        fi
    }
```

Appendix B

SPIN State Diagram

(i) For proactive protocol

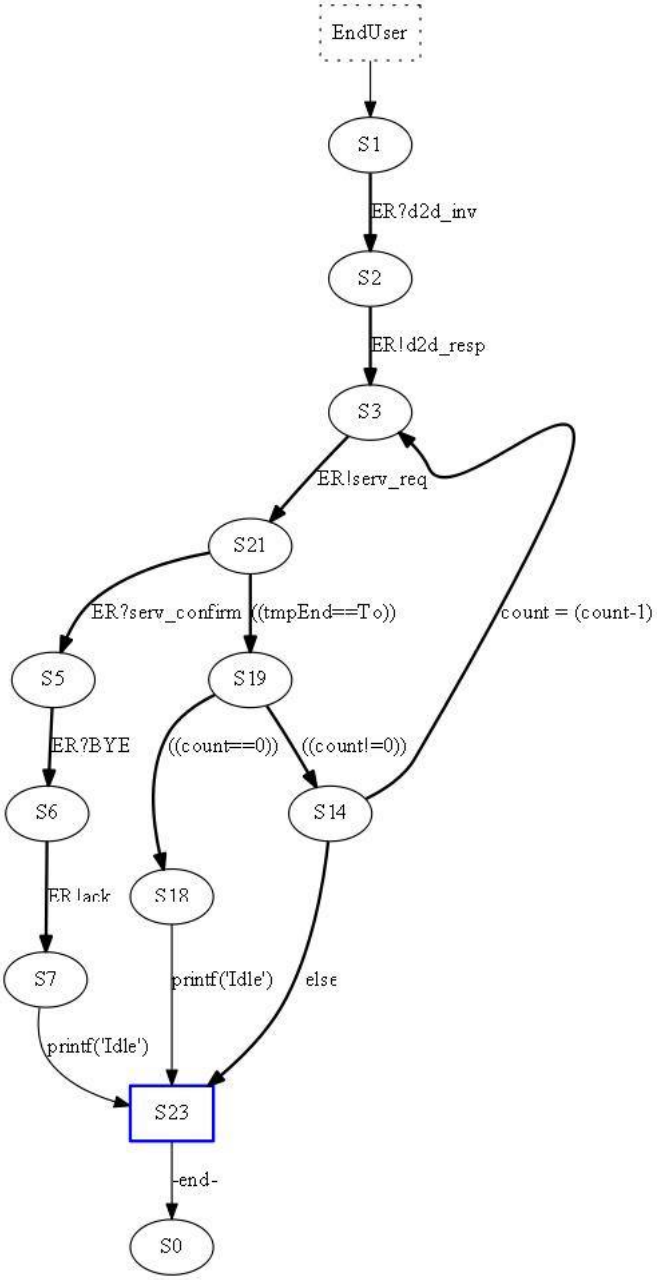


Figure B.1: State diagram from UE-E's prospective for proactive protocol.

(ii) For reactive protoccol

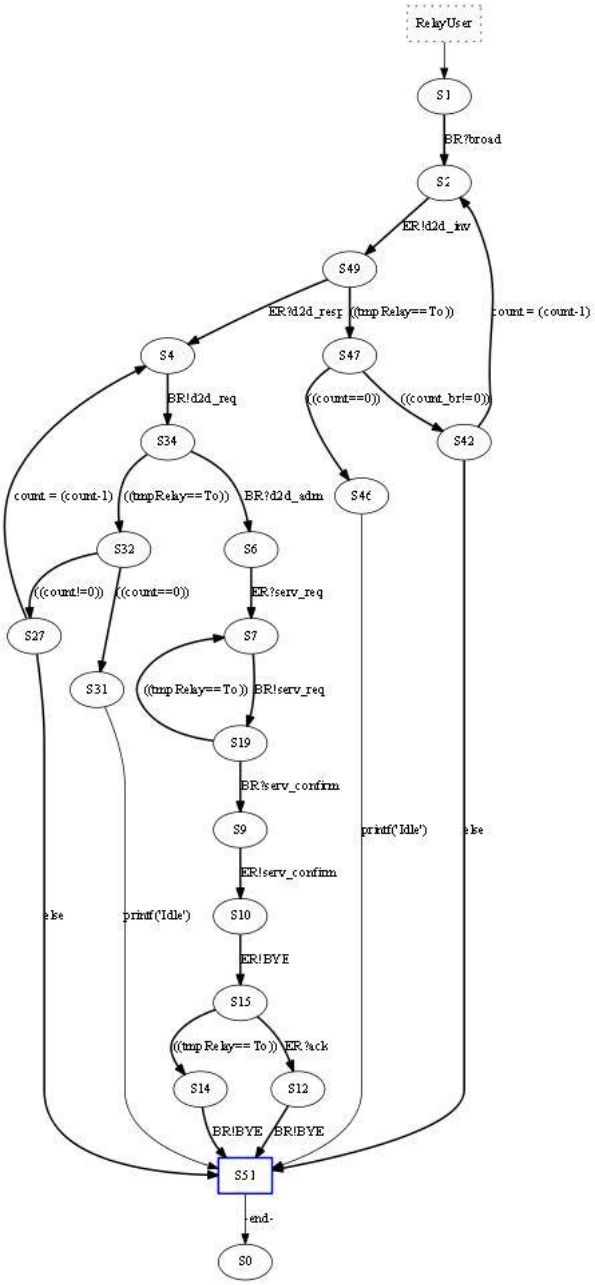


Figure B.2: State diagram from UE-R's prospective for proactive protocol.

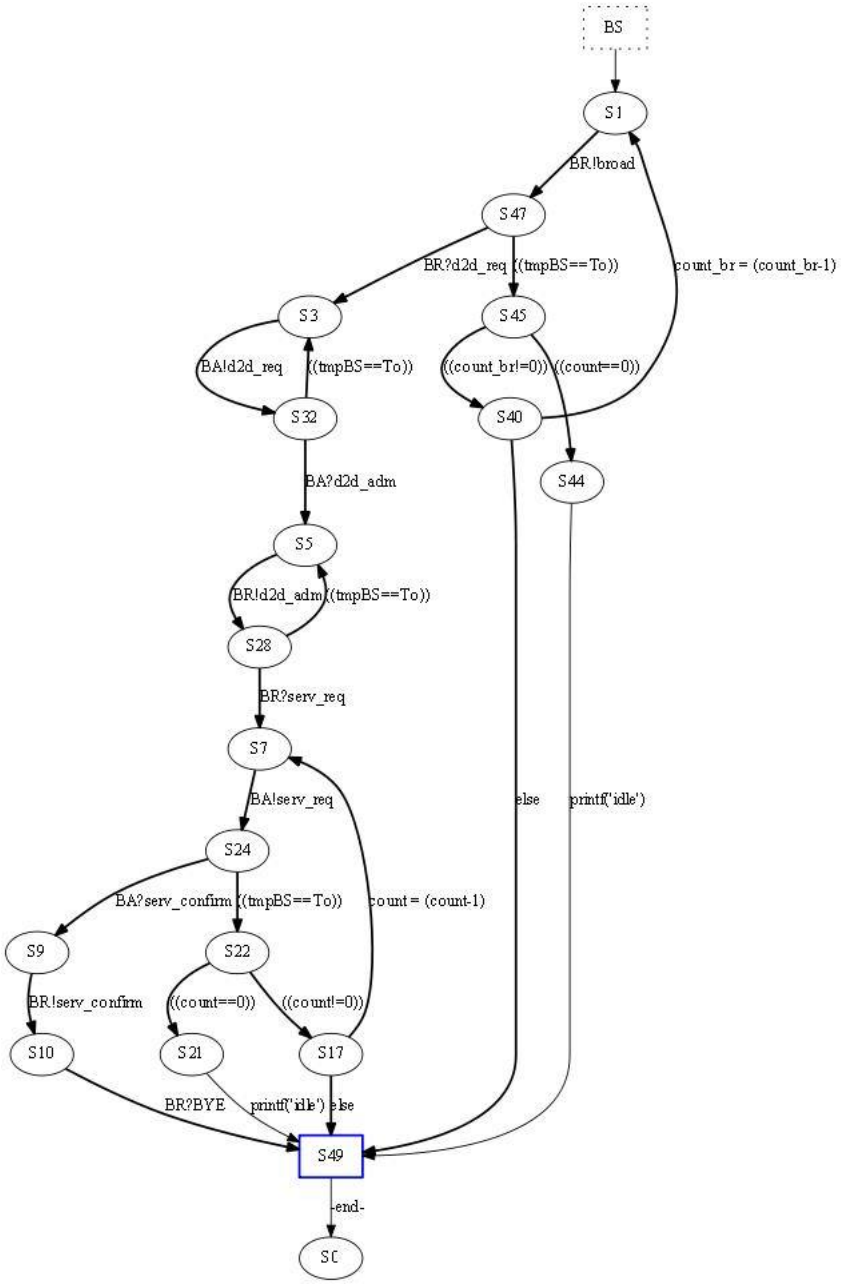


Figure B.3: State diagram from BS's prospective for proactive protocol.

(iii) For security enhancement Protocol

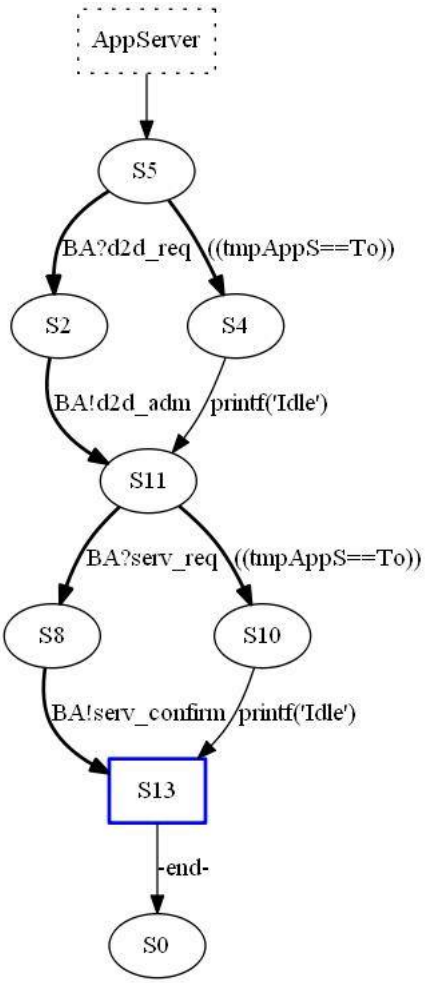


Figure B.4: State diagram from AS's prospective for proactive protocol.

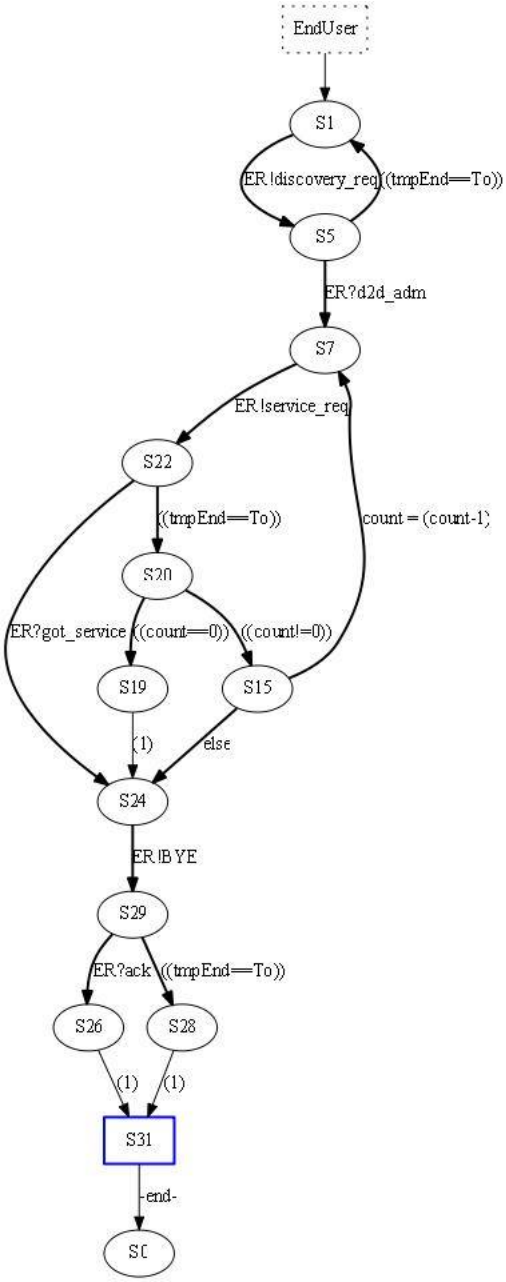


Figure B.5: State diagram from UE-E's prospective for reactive protocol.

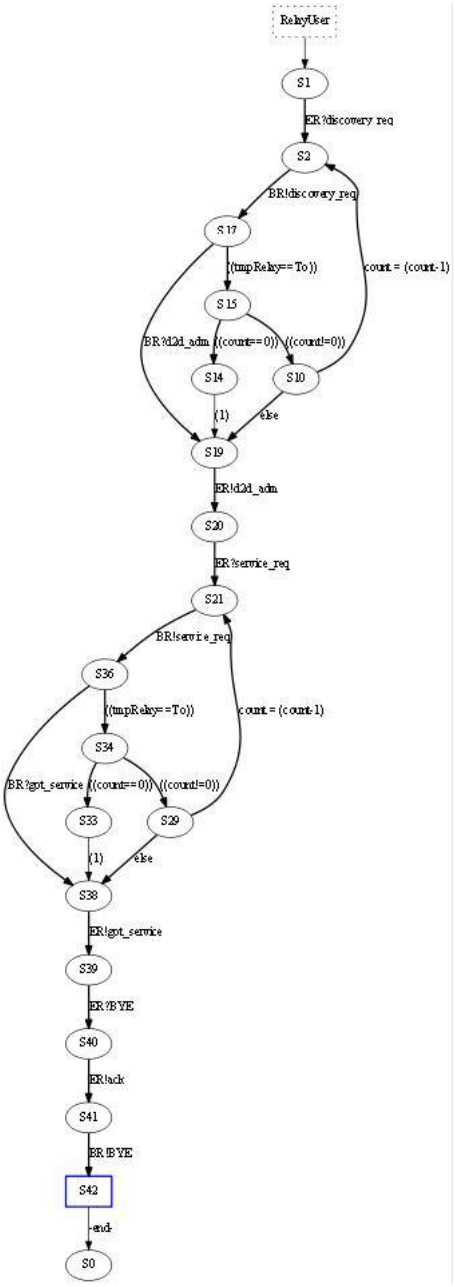


Figure B.6: State diagram from UE-R's prospective for reactive protocol.

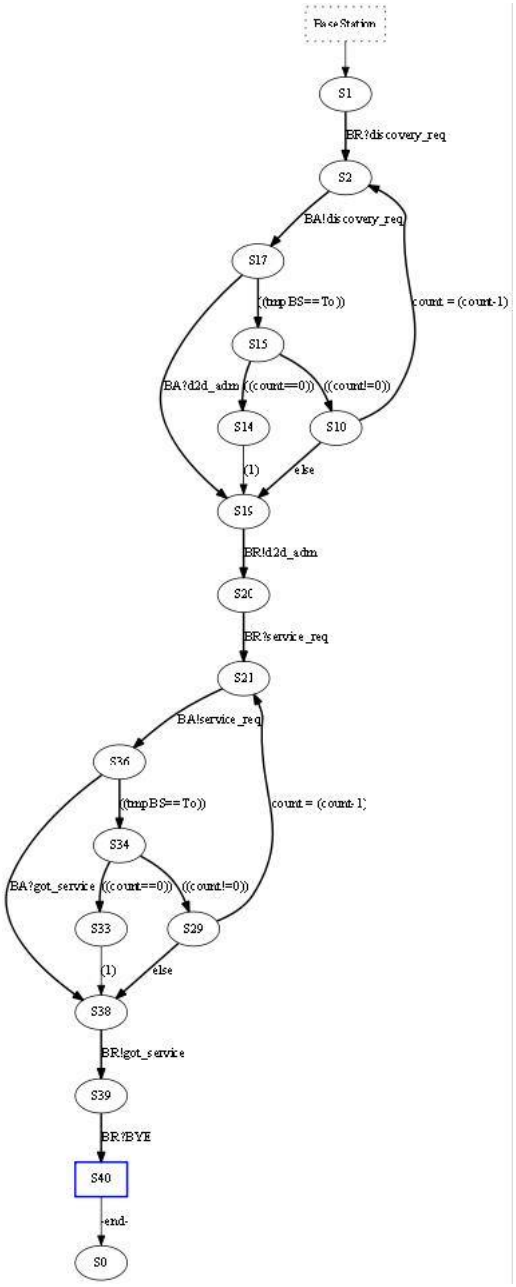


Figure B.7: State diagram from BS's prospective for reactive protocol.

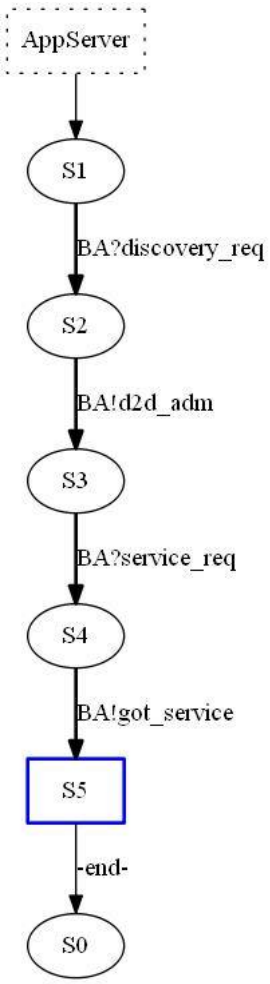


Figure B.8: State diagram from AS's prospective for reactive protocol.

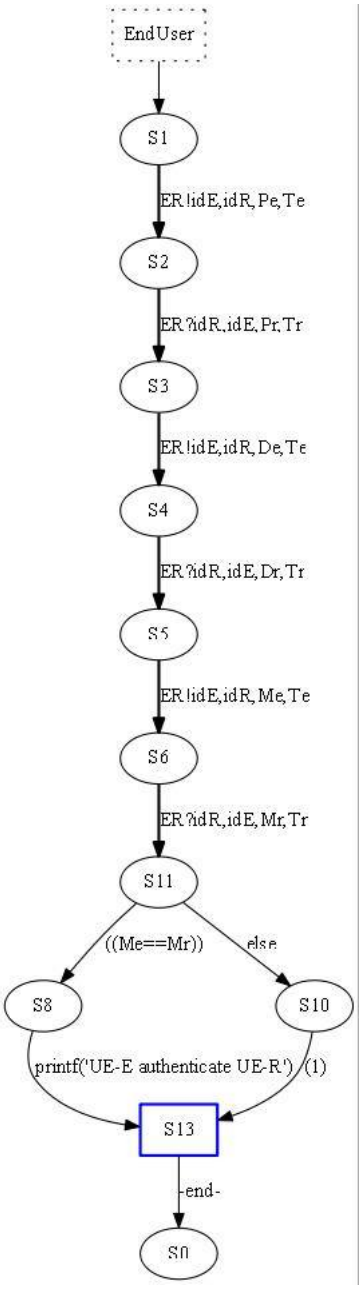


Figure B.9: SPIN state diagram from UE-E's prospective for security enhancement protocol.

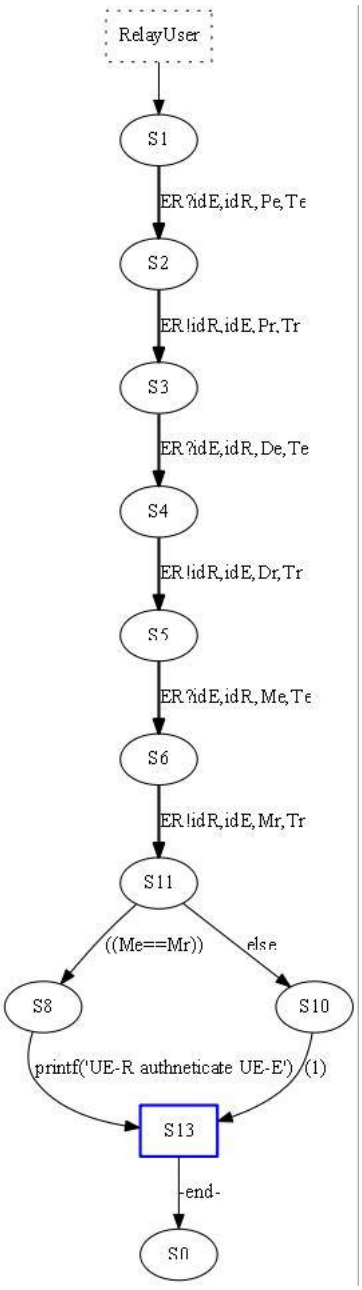


Figure B.10: SPIN state diagram from UE-R's prospective for security enhancement protocol.

Appendix C

MATLAB Code

(i) Control overhead calculation for both protocol when D2D request is normally distributed

```
Sig=2.14;                 %Standard deviation
mu=3.8;                   %Mean
T=20;                     % Total timeslot
K=20;                    %Total timeslots at which D2D request occurs
M=mu+Sig*randn(1,K);     %Normally generated random number
TH1=K*(2+(14*M));        %Total handshake for Proactive protocol
TH2=(K*15*M);            %Total handshake for reactive protocol
CO1=(2*(T-K)+TH1)./T;    %Control overhead for proactive protocol
CO2=TH2./T;               %Control overhead for reactive protocol
hold on
plot(M,CO1,'-^',M,CO2,'-o');
legend('Proactive, D2D','Reactive,D2D');
xlabel('Normally Generated D2D Request');
ylabel('Control overhead for Normally Generated D2D Requests');
title('Control Overhead Vs Number of D2D Request');
grid on;
```

(ii) Control overhead calculation for both protocol when D2D request is same at each timeslot

```
T=20;                   %Total timeslot
M=5;                    %D2D request at each timeslot
K=1:1:20;               %Total timeslot at which D2D request occurs
TH1=(2+(14*M));         %Total handshake Proactive protocol per one timeslot
TH2=(15*M);             %Total handshake reactive protocol per one timeslot
CO1=(K*TH1+(2*(T-K)))/T;  %Control overhead for Proactive protocol
CO2=(K*TH2)/T;             %Control overhead for reactive protocol.
plot(K,CO1,'-*',K,CO2,'-^');
```

```
legend('Proactive','Reactive');
xlabel('Number of Timeslots at which D2D Request Occurs');
ylabel('Protocol Overhead (number of handshakes per timeslot)');
title('Protocol Overhead vs Number of Timeslots with D2D Request');
grid on;
```

(iii) Control overhead calculation for both protocol when D2D request is different at each timeslot

```
d=0:10:100;  % Allowable distance for D2D communication
D=100;       %Maximium distance betwwen UE-R and UE-E.
N=15;       %Total number of UE-E in the area not covered by cell
n=10;       %Number of UE-E user with Prose services among N user.
R=1000;     %Radius of the Netowork coverage cell.
r=980;
h=20;
z=h*(2*R-h);
a=2*sqrt(z);
A1=square(R)*acos((R-h)/R);
A2=pi*(D^2)/2; %Area of semi circle covered by UE-R
A=A2-A1;         %Area lies outside network coverage cell
lembda=N/A;      %UE-Es density
P=1-exp(-lembda*pi*(d.^2)); %Proximity probability PPP distribution.
K=14; % Total timeslots at which D2D requests occur.
M=0:1:10; %Random number od D2D requests
T=20; %Total timeslot
t=9;
for i=0:t

        Y = 1-binocdf(i,n,P);
        i=i+1;

end
TH1=(2+(14*M)); %Total handshake for Proactive protocol
TH2=(15*M); %Total handshake for reactive protocol
CO1=(K*TH1+(2*(T-K)))/T; %Control overhead for Proactive protocol
CO2=(K*TH2)/T; %Control overhead for reactive protocol.
CO1=Y.*CO1;
CO2=Y.*CO2;
plot(d,CO1,'-*',d,CO2,'-^');
legend('Proactive','Reactive');
xlabel('Target distance, D (m)');
ylabel('Protocol overhead (Total number of handshake per timeslot)');
title('Protocol overhead vs. target distance (m)');
grid on;
```

(iv) Proximity probability for at least k number of D2D request

```
D=100;      %maximium distance betwwen UE-R and UE-E.
d=1:10:100; %Targeted distance between UE-E and UE-R.
N=15;       %UE-Es outside coverage area
%n=1:1:10;   %Number of UE-E user with Prose services among N user.
r=980;          %Distance between BS and UE-R.
h=20;           %Distance between edge of network coverage and UE-R
z=h*(2*R-h);
a=2*sqrt(z);    %Length of chord inside coverage cell.
A1=square(R)*acos((R-h)/R); %Area of sector inside cell
A2=pi*(D^2)/2;%Area of the semi circle covered by UE-R
A=A2-A1;       %Area outside cell covered by UE-R
lembda=N/A;     %UE-Es density outside cell
P=1-exp(-lembda*pi*(d.^2));%Proximity probability in given area..
k0=9;                       %Number of UE-E outside coverage area
k1=7;
k2=5;
k3=3;
k4=1;
Y0=1-binocdf(k0,n,P); %Probability at which atleast one UE-E send request
Y1=1-binocdf(k1,n,P);
Y2=1-binocdf(k2,n,P);
Y3=1-binocdf(k3,n,P);
Y4=1-binocdf(k4,n,P);
plot(d,Y0,'-kv',d,Y1,'-o',d,Y2,'-^',d,Y3,'-*',d,Y4,'-x');
legend('P(k=9)','P(k=7)','P(k=5)','P(k=3)','P(k=1)');
xlabel('Distance between UE-R and UE-E');
ylabel('Probability of k UE-E to be D2D pair with UE-R');
title('Probability of atleast k UE-E send request vs Proximity distance');
grid on;
```