Journal of Engineering Design and Analysis
Volume 3, Issue 2 - 2020, Pg. No. 72-72
Peer Reviewed Journal

Review Article

Document Analysis of Efficient Group Key Management using D2D Communication

Ezekiel U Okike[1], Boleng Ratlhako[2]

[1,2]University of Botswana, Gaborone, Botswana.

INFO

Corresponding Author:
Ezekiel U Okike, University of Botswana, Gaborone, Botswana.
E-mail Id:
euokike@gmail.com

How to cite this article:
Okike EU, Ratlhako E. Document Analysis of Efficient Group Key Management using D2D Communication. *J Engr Desg Anal* 2020*;* 3(2): 72-77.

Date of Submission: 2020-11-03
Date of Acceptance: 2020-11-20

ABSTRACT

The availability of smartphones and tablet subscribers has brought improvements in wireless cellular networks through Device-to-Device (D2D) communications. However, addressing security challenges in D2D communication is still a research problem, especially, the Data Transformation Phenomenon (DTP) which affects the performance of Group Key Management (GKM) In this paper, we present a document analysis of the main factors required for efficient group key management, and proposal a scenario based approach for finding appropriate solution which uses a D2D communication in GKM to improve the DTP by presenting a light, secure and resilient environment.

Keywords: D2D Communication, Data transformation, Group key management, Security

Introduction

Device-to-Device (D2D) communication, also known as mobile to mobile communication, refers to a radio technology that enabled devices to communicate directly with each other, that is without routing the data paths through a network infrastructure. Device-to-Device communication is a new technology that offer many advantages for the Long Term Evolution (LTE) advanced network such as wireless peer-to-peer services and higher spectral efficiency.[3,4] It is also considered as one of promising techniques for the 5G wireless communications system and used in so many different fields such as network traffic offloading, public safety, social services and applications such as gaming and military applications. D2D communications was initially proposed in cellular network as a new paradigm to enhance network performance.[11]

The emergence and popularity of personal mobile devices, such as smartphones and tablets, generates large amount of data traffic by accessing the Internet and downloading applications, which imposes a huge burden for the cellular infrastructure and spectrum. D2D communications have been introduced to offload the traffic burden from cellular infrastructure to personal devices.

Though Device-to Device communication has been a hot research topic in recent years, there is not much study focusing on the security aspect of D2D communications.[1,2] discuss the physical layer solutions for secure D2D communications, but their techniques are difficult to be implemented using devices on the market.

Accordingly, due to the broadcast nature of wireless communication, wireless channels are considered vulnerable to a variety of attacks, and security is one of the major concerns for D2D communications. To secure the communication between two end users of a D2D link, establishing a shared secret key is the first and most significant step. However, lack of trusted third party and infrastructure under D2D connection environment makes this step a non-trivial task. This proposal takes advantage of the benefits of the D2D mechanism to build an efficient group key management (EGKM) scheme.

Statement of the Problem

Despite all the benefits of D2D communications, security is one of the major concerns that need to be well addressed before D2D technique gets widely accepted and implemented. It is well known that due to the broadcast nature of wireless channels, wireless communication such as Wi-Fi and Blue tooth is vulnerable to a variety of attacks that challenge the three basic principles of security Confidentiality, integrity and availability. Some common attack vectors include surreptitious Eavesdropping , message modification and node impersonation. For example, by stealthy listening to the communication between two devices, an attacker can gain critical or privacy information, such as trade secrets or identity related information. Thus, the D2D communications between devices need to be properly secured.

Objectives

The objective of this paper is to present a document analysis of efficient Group Key Management techniques in Device-to-Device (D2D) communication, and to recommend appropriate security measures in D2D communication.

Methodology

A Document Analysis and Perusal (DA&P) approach was adopted by consulting a wide range of literatures on the subject of Device-to-Device (D2D) communication and Group Key Management (GKM) for broader and updated view of the current situation while searching for appropriate solution to the problem on hand. After thorough literature analysis and objective critique, appropriate recommendation for efficient GKM were arrived at.

Literature Review

Device-to-Device Communication

The motivation for D2D came directly from both the perceived user requirements, as well as the system requirements for D2D communications of the future. These requirements include new types of short range services and data intensive short range applications.[5] The emergence of context-aware and multimedia applications have also constituted to the motivation of using D2D technology. Expectedly, D2D communications should allow new types of services such as multimedia downloading, video streaming, online gaming and peer-to- peer (P2P) file sharing.

As a technology that enable the communication between multiple devices or users without having base station or intermediary devices on a network, D2D communication is a key technology to solve problems such as coverage and interference management.[6] Other advantages of this technology is the fact that it increases the spectrum utilization and capacity enhancement of network performance and throughput. Differing from the Bluetooth and WiFi-direct technologies, D2D communication may be the defacto standard communication in cellular network technology based on the spectrum in which D2D communications occurs. Thus, D2D communication can occur on cellular system and in this case called Inband D2D or can occur in unlicensed spectrum in which case it is called Outband D2D. In D2D communications the cellular network can handle phone calls and internet data traffic without additional networks load from the promotional material. However, there are many complexities of setting up and to deploy D2D communications in LTE advanced networks. These challenges and complexities include:

- D2D devices cause interference to the cellular users which affect the performance of the network devices.
- D2D communications define new QoS requirements that must be addressed.

Hence, LTE-advanced present two techniques of D2D communications that use Session Initiation Protocol (SIP) and Internet Protocol (IP). These techniques have the benefit of providing the control over the D2D connectivity to the operator. The integration of D2D communications in LTE-A must take into account LTE-A interfaces and network elements.

While the need for physical layer backward capability imposes the D2D devices to utilize for their links the current structure of the spectrum resources.

Classification of D2D Communication

D2D communication in cellular network can be categorized into both Inband D2D and Outband D2D based on the spectrum in which D2D communications occurs. D2D communications is divided into two modes or categories called ‘Inband underlay mode’ when the D2D communications use the cellular resources and spectrum and ‘Inband overlay mode’ when cellular resources are allocated for the two D2D end devices that communicate directly (e.g. Figure 1) .

High control over licensed spectrum is the key motivating factor for choosing the Inband D2D communication. On the other hand, the main motivation of using Outband D2D communications is the capacity to eliminate the interference between D2D links. Furthermore, Outband D2D communications is faced with a lot of challenges in the coordination between different bands. Figure 1 below shows the basic classification of D2D communication.

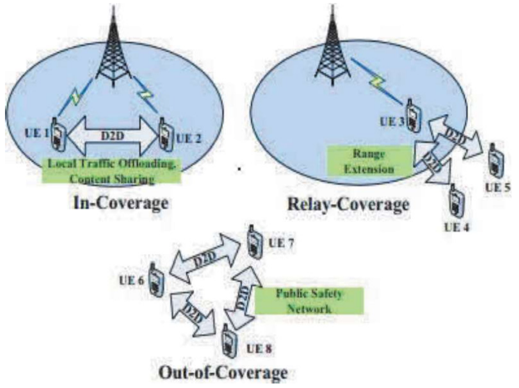

Figure 1.Classification of D2D communication

Application Scenarios and Use Case

The application scenarios and use cases of D2D communications have been explored as an underlay of a cellular network or a national security and public safety network. They are categorized into three representative types according to the involvement of various network entities (i.e., cellular base stations and core networks) and the type of utilized spectrum resources,[7] as illustrated in Figure 2.

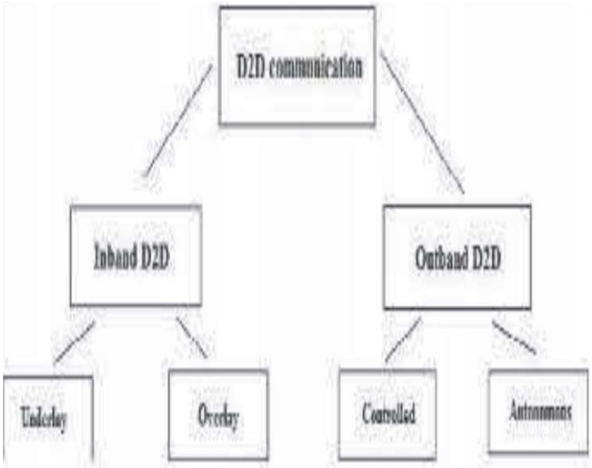

Figure 2.D2D Communication application scenarios and use cases

In-Coverage: in this scenario, user devices (e.g. UE1 and UE2) are located in the coverage of cellular BSs, D2D communications between two user devices are fully controlled by network entities, such as base stations or core networks. The operator controls over user access authentication of D2D communications, connection establishment, resource allocation and security management. This kind of D2D link shares the cellular licensed spectrum with the normal cellular connections (Device-to-Base Station) under the coordination of an operator. Typical use cases of this scenario are local traffic offloading from the core networks and operator controlled local data services, such as local content sharing, machine to machine (M2M) communications.

Relay-Coverage: when a user device (e.g. UE4 and UE5) is at the edge of BS coverage or in a poor coverage area, it can communicate with the BS through relaying its information via other covered devices (e.g. UE3). The introduction of D2D communications can greatly extend the coverage of cellular networks and improve the Quality of Services at a cellular edge. This type of D2DCommunications is defined as "relay coverage" Scenario. In this case, like the "In-Coverage" scenario, the operator is fully in charge of link establishment for both BS-to- device link and D2D link, resource allocation (especially for the D2D link) and security management. The band used in the D2D link in this scenario is also the cellular licensed spectrum shared with conventional communications.

Out-of-Coverage: another representative application scenario of D2D communications occurs when the network coverage is absent. A Typical use case of "out-of-Coverage" is Emergence Communication Networks.

For example, in an emergent situation where the cellular infrastructure has been partially or completely damaged due to natural disaster (e.g., earthquake or flood), D2D devices (e.g. UE6, UE7 and UE8) can setup connections and start D2D communications autonomously with others in proximity without the control of any operators. As studied in[8,9] this D2D communication scenario can serve as a technical component for providing services such as public protection, disaster relief, national security and public safety. This D2D communication scenario looks similar to Mobile Ad-hoc Networks (MANET). However, their key difference lies in D2D link works on a reserved cellular licensed spectrum for an LTE-based public safety network, while MANET works on unlicensed Industrial, Scientific and Medical (ISM) spectrum, which make it under more severe interference comparing with D2D communications.

Device To Device Communication Security

Despite all the benefits of D2D communications, security is one of the major concerns that need to be well addressed before D2D technique gets widely accepted and implemented. It is well known that due to the broadcast nature of wireless channels, wireless communication such as Wi-Fi and Blue tooth is vulnerable to a variety of attacks that challenges the three basic principles of security confidentiality, integrity and availability.

Some common attack vectors include surreptitious Eavesdropping, message modification and node impersonation. For example, by stealthy listening to the communication between two devices, an attacker can gain critical or privacy information, such as trade secrets or identity related information. Thus, the D2D communications between devices need to be properly secured.

Requirements of D2D Communication Security

In order to resist the potential security threats on D2D communications, below are the security requirements that a D2D communication system should satisfy.

Confidentiality and Integrity (C\ I): In order to prevent control signaling and user data from maliciously modifying and leaking during transmission, the data needs to be always kept confidential and integrated. For example, in the Relay Coverage scenario, a receiver can detect any accidental or malicious data alteration by a relay device. All the security domains in D2D communications should support the confidentiality and integrity of data transmission, especially for control signaling.

Authentication (Au): Authentication is the cornerstone of correct functioning of the whole D2D communication system. It is the key to resist the impersonate attack. It must be possible to verify the eligibility of a device or an application to use a D2D service, which is performed on PC1, PC2 or PC3. Meanwhile, the D2D user should be able to verify the identity of D2D service provider. In order to guarantee the security of data transmission, it should be also possible to verify the identity of the sender of any message exchanged in the D2D network, which may happen on PC5. Since the D2D communications relate to relay communications and fully distributed communications, user identity authentication are totally different from common authentication schemes. New authentication schemes for D2D communications are needed, especially a uniform scheme that is applicable in D2D communication scenarios.

Fine-grained Access Control (FAC): Fine- grained refers to the small granularity of an access policy, which could take into account a user's personal profile and other factors. For example, the D2D application servers always perform access control to D2D devices on their services and data based on fine-grained policies. Moreover, FAC is also expected for group communications, which is an application scenario in D2D communications. Fine-grained data access control needs to be enforced for data delivery in D2D communications so that unauthorized users cannot obtain private information.

Privacy (Pr): User identity, location and other personal information must be concealed to non- authorized parties. Comparing with data confidentiality, user data privacy concerns more about the D2D service functionalities in order to control data leakage to any other parties except the data owner.

Non-Repudiation (NR): To be able to find and separate compromised devices, it must be impossible for a sender or a receiver of a message to successfully deny the authorship or reception of that message.

Revocability (Re): It is indispensable to revoke the user privilege of a D2D service if a user is detected as malicious or harmful or out of service.

Availability and Dependability (A\D): The D2D services should be always available even under attacks such as DoS or DDoS attacks. Intermittent unavailability of the D2D services may irritate user experiences thus hinders the adoption of D2D communications.

Security Threats in D2D communications

New functional entities and reference points for implementing D2D communications introduce new security threats comparing with traditional cellular communication systems (e.g. LTE networks). Except for the traditional security issues in LTE networking, there are a number of D2D specific threats that stem from the particularities of the D2D architecture and its security model. Below are the main security threats specifically relevant to D2D communications.

Impersonation Attack In the out-of-coverage scenario, a malicious user can easily create multiple fake identities and impersonate legitimate users to communicate with other users due to the absence of the core infrastructure.

Threats related to Data Transmission Security The communication data, which includes user data and control signaling, are subjected to eavesdropping, fabrication and manipulation during transmission among all system entities.

Threats due to user devices mobility Mobility brings additional challenges on the continuity of the D2D communication security.

Threats against Privacy User personal information could be disclosed in D2D communication.

To secure the D2D communications, cryptography solutions are needed to encrypt the messages while they are transmitted via wireless channels. Numerous encryption algorithms have been well developed which can provide different security levels for the encrypted messages, but all of them require two devices agree on a shared secret (either a shared secret key or each other's public keys) Due to the large number of mobile devices, the diversity of device manufacturers and lack of standards, preloading secure keys into mobile Devices is neither efficient nor practical. On the other hand, a trusted third party or infrastructure is not likely to be available in the D2D mobile environment. Thus, how to establish a shared secret between devices is one of the main challenges for secure D2D communications.

Group Key Management

For securing any group communication like multicast architectures, there is a need to build a strong protocol for the Group Key Management (GKM). Group communication has two important Security requirements: "Group Confidentiality" and ' key Management'. Furthermore, the security of established sessions must be guaranteed. Therefore, it can be conclude that; the base for providing common security services for group Communication is the 'Key Management' 10.

Group key Management has very simple usage but it suffers from two problems: the problem of keys distribution and the problem of keys revocation. Thus, the security issues for building a secure group communication have two types: security requirements in GKM and QoS.

GKM Security Requirements

The five security requirements in GKM: forward secrecy, backward secrecy, collusion freedom, Key Independence and Trust Relationship. All those security requirements can be defined as follows:

Forward Secrecy (FS): for users who left the group, they should not have an access to the future key.

Backward Secrecy (BS): for new users who join the session, they should not have an access to the old key.

Collusion Freedom (CF): for any set of fraudulent users, they should not be able to deduce the current traffic encryption.

Key Independence (KI): for different groups (i.e different ProSe(s)) keys must not be able to discover any other group key.

Trust Relationship (TR): for not revealing the keys to any other part (same domain) or party (another domain).

Ways to Establish a Shared Secret

To secure the D2D communications, cryptography solutions are needed to encrypt the messages while they are transmitted via wireless channels. Numerous encryption algorithms have been well devel-oped which can provide different security levels for the encrypted messages, but all of them require two devices agree on a shared secret (either a shared secret key or ither's public keys).

Due to the large number of mobile devices, the diversity of device manufacturers and lack of standards, preloading secure keys into mobile Devices is neither efficient nor practical. On the other hand, a trusted third party or infrastructure is not likely to be available in the D2D mobile environment. Thus, how to establish a shared secret between devices is one of the main challenges for secure D2D communications.

One straightforward way to establish a shared secret between two devices is that the two end users of the D2D link interactively set up a secret key via human negotiation (such as making a phone call if they are in distance). The problem for this is that the shared secret established by human interaction will be too weak in most cases. The attackers do not even need to be smart to crack this weak secret via brute force method, considering current computation power. To deal with this issue, cryptologists and researchers come up with two types of approaches which enable two individuals to establish a secure enough secret key: Diffie-Hellman key establishment protocol and secret key extraction from physical channel characteristics.

Physical layer based secret key generation methods have been proposed in recent years as alternative solutions for traditional Diffie-Hellman key agreement protocol, whose security is guaranteed by the computational hardness of discrete logarithms, these physical layer based methods rely on the ran-domness and uniqueness of wireless fading channel properties: temporal variation, spatial variation and uniqueness of the wireless fading channel properties: temporal variation, spatial variation and reciprocity. Generally, the two devices first send channel probing packets to measure the physical metrics of the wireless channel, then after using quantization and error correction technique, these two de-vices can yield the same secret key. The main problem for this type of methods is that the secret key generation rate is in most case very low. Users have to send lots of channel probing packets to achieve a secret key with enough bits and randomness. The communication overhead and relatively longer key generation time are not quite desirable for the case of D2D communications.

Diffie- Hellman cryptosystem is the oldest public key system still in use, which allows two individuals to agree on a shared secret key, even though they can only exchange messages over public channels. Implantation of Diffie-Hallman key agreement protocol requires some extent of computation capacity. However, mainstream mobile devices on today's market have achieved gigahertz level processor fre-quency, so generating a secure enough shared secret, say, 156 bits, can be conducted within seconds.

Conclusion and Reccommendation

Consider the following scenario: Two mobile device users want to establish a D2D communications. Both of them are equipped with a smart phone or tablet which is capable of communicating over a wireless channel. Both devices have the computation capacity to perform Diffie-Hellman key agree-ment protocol, and are capable of displaying sequence of digits. The two users have pre-shared cryp-tographic information. They can visually or verbally recognize each other for the purpose of mutually authenticating a short message. The Data Transformation problem causes significant performance overheads in group key management and this is not suitable for real time computing. How does D2D communication resolve or reduce Data Transformation problem in group key management?

The performance overheads of the newly proposed will be based on the following metrics or complex-ities;

- Communication Complexity
- Storage Complexity
- Transmission Complexity
- Computation Complexity

Conclusion

Device-to-Device (D2D) communications have been treated as a promising technical component for 5G. In spite of impressive benefits, D2D communications encounter many security problems. Howev-er, D2D security hasn't yet been seriously investigated in both academic and standardization communi-ties. Research has shown the main D2D application scenarios and use cases. Research has further pro-posed a D2D security architecture compatible with the LTE system and suggested D2D security re-quirements accordingly. Based on the security architecture and security requirements, the existing work has been reviewed in order to explore open research issues and propose future research direc-tions. It is recommended that significant efforts are needed in order to overcome D2D security prob-lems in particular the data transformation problem in group key management.

References

1. Wang J, Li c, Wu j. Physical LAYER security of D2D communications under layer cellar networks. *Applied Mechanics and Materials* 2014; 441: 951-954.
2. Zhu D, Swindlehurst AL, Fakoorian SA et al. Device-to-Device communications: the physical layer security advantage. In IEEE ICASSP, 2014.
3. Harsha ES, Tirupa T. Advanced cellular networks for D2D communications. *International Journal of Scientific Engineering and Technology Research* 2014; 3(18): 2014.
4. Asadi A, Wang Q, Mancuso V. A Survey on Device-to-Device Communication in Cel-lular. Netwoks arXiv: 1310.0720v6[cs. GT] 29April2014.
5. Tsolkas D, Liotou E, Passas N et al. LTE-A Access, Core and Protocol Ar-chitecture for D2D communication. *Springer International Publishing Switzerland* 2014.
6. Lin Z, Gao Z, Huang L et al. Hybrid Architecture Performance Analysis for Device-to-Device Communication in 5G cellular Network. @ Spriger Science+Business Me-dia New York 2015.
7. Mingjun W, Zheng Y. Security in D2D Communication. Xidian University, Xi'an, *China* 2015.
8. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-based services (ProSe); Stage 2 (Rel 12) 3GPP TS 23.303 V12.0.0 2014-12.
9. Fodor G, Parkvall S, Sorrentino S et al. Device-to-Device communication for national security. Institut Mines telecom RST Department Saclay, *France* 2015.
10. Arash A, Qing W, Mancuso V. Device-to-Device Communic ation in Cellular networks. *IEEE communication survey and tutorials* 2014; 16(4): 1801-1819.