Security in Network Services Delivery for 5G enabled D2D Communications: Challenges and Solutions*

Ed Kamya Kiyemba Edris[1][0000−0001−5981−9844], Mahdi Aiash[1][0000−0002−3984−6244], and Jonathan Loo[2][0000−0002−2197−8126]

[1] Middlesex University, London, United, Kingdom
ee351@live.mdx.ac.uk, m.aiash@mdx.ac.uk
[2] University of West London, London, United Kingdom
jonathan.loo@uwl.ac.uk

Abstract. Due to the increasing data traffic in mobile network, fifth generation (5G) will use Device to Device (D2D) communications as the underlay technology to offload traffic from the 5G core network (5GC) and push content to the edge closer to the users by taking advantage of proximity and storage features of User Equipment (UE). This will be supported by Networks Services (NS) provided by 5G, it will also enable new use cases that will provide the accessibility to other services in the Home network (HN) and third-party service provider (SP). Mobile Network Operators (MNO) will use NS such as D2D communications and content-centric networking (CCN) to deliver content-based services efficiently to UE. Both D2D and CCN have known security issues and their integration brings new security challenges. In this article, we present an integrated network service delivery (NSD) framework for 5G enabled D2D communications that leverages on NS for service discovery, content delivery, and protection of data. We also present a comprehensive investigation of security and privacy in D2D communications and service-oriented network, highlighting the vulnerabilities and threats on the network. We also evaluate the security requirements of NSD to deliver NS securely to D2D users based on X.805 security framework using the eight security dimensions and level abstraction approach for a systematic and comprehensive approach. Finally, we recommend security solution approaches for the secure NS access and sharing of data between users in 5G enabled D2D communications network.

Keywords: 5G · Survey · Network services · Security analysis· Content sharing · Service delivery · Device-to-device · Content-centric · X.805 framework.

1 Introduction

Over the past few years there has been an increase in the mobile traffic due to rising demand of over-the-top applications (OTT) such as social media, live

* Supported by organization x.

streaming, local based advertising, and popularity of smart phones usage [15]. Mobile traffic is anticipated to keep growing gradually, most of traffic is from mobile devices and Machine to Machine communications (M2M) [17]. The demand of multimedia contents and expectation of high availability and performance by the end users affected the network capacity. Whereby network infrastructures were overloaded and became highly inefficient for content distribution [38]. Most of the data traffic load of the mobile network backhaul is generated from the mobile user's traffic. The fifth-generation mobile network (5G) was inspired by the need for very high reliability, ultra-low latency network to support services and the increasing demand of quick access and delivery of data by end users and Mobile Network Operators (MNO) [30]. 5G will enable the end users to be involved in content-based operations through Device to Device (D2D) communications, which will enhance user's experience. D2D Communications will be used as an underlay technology for 5G to offload traffic from the network backhaul by pushing content to edge closer to the end users [31]. D2D communications will also be fundamental to the implementation of Internet of Things (IoT). Content distribution and retrieval will dominate mobile traffic, however delivering such services to the end user efficiently and securely is becoming a big challenge.

D2D communications [2] was specified by the Third Generation Partnership Project (3GPP) with a purpose of network offloading via the User Equipment (UE) by communicating directly without conveying content through the Base Station (BS). In 5G, the UE will act as a data consumer as well as playing a role in content distribution and delivery [1]. 5G enabled D2D communications will support new use cases and services, the delivery of these services to the end user will be facilitated by Network Services (NS) by using context aware enabled devices. To be able to distribute and deliver contents to the end user various content delivery models such as Content Delivery Network (CDN) [38] will be used. CDN can be deployed at edge, BS, and access points to support cache servers and with D2D communications, mobile devices can also be used as cache nodes [28]. Most of the wireless traffic generated in cellular network is from the downloads of popular content replicated in multiple locations [47]. The introduction of CDN and content caching in mobile network can be integrated with Information-Centric Networking (ICN), transforming the network from connection centric to information centric such as Content-Centric Networking (CCN) [36] in next generation mobile network [41].

Due heterogeneous nature of 5G, UE, network and the data will be vulnerable to new and old attacks when UEs are accessing services in the Home Network (HN) and third-party service provider (SP). In addition, UEs sharing continent in out of coverage scenario without control of the network will need robust protection. So far, less attention has been given to the security issues faced by an integrated service framework for mobile network as the one presented in this article. To best of our knowledge no study has been carried out so far to investigate the security threats and requirements of Network Service Delivery (NSD) in 5G enabled D2D communications, using a systematic approach, moreover there is need for a security framework for NSD. The provision of secure NSD is essential to achieving the main objectives of 5G.

The study is motivated by a secure NSD in 5G enabled D2D communications leveraging on other NSs for service discovery, content delivery, and protection of data. The emphasis is on the protection of data and communication channels from different threats. To give a systematic approach of the security evaluation for 5G enabled D2D communications, we apply the X.805 security framework [73] with NS abstraction level approach [20]. This framework has been used to evaluate end to end security of communication centric systems such as 4G [55], internet of things [57], and ICN [49].

The article adds the following contributions: firstly, it presents a NSD framework for delivery and sharing services between UEs in different scenarios. Secondly, it comprehensively investigates of security and privacy of 5G enabled D2D communications network. It identifies the potential threats against D2D communications and ICN integrated system model. Thirdly, it evaluates the security requirements using a systematic and abstract approach for more comprehensive evaluation using X.805 framework. Lastly, suggests possible solutions of the threats and mention future work on NSD.

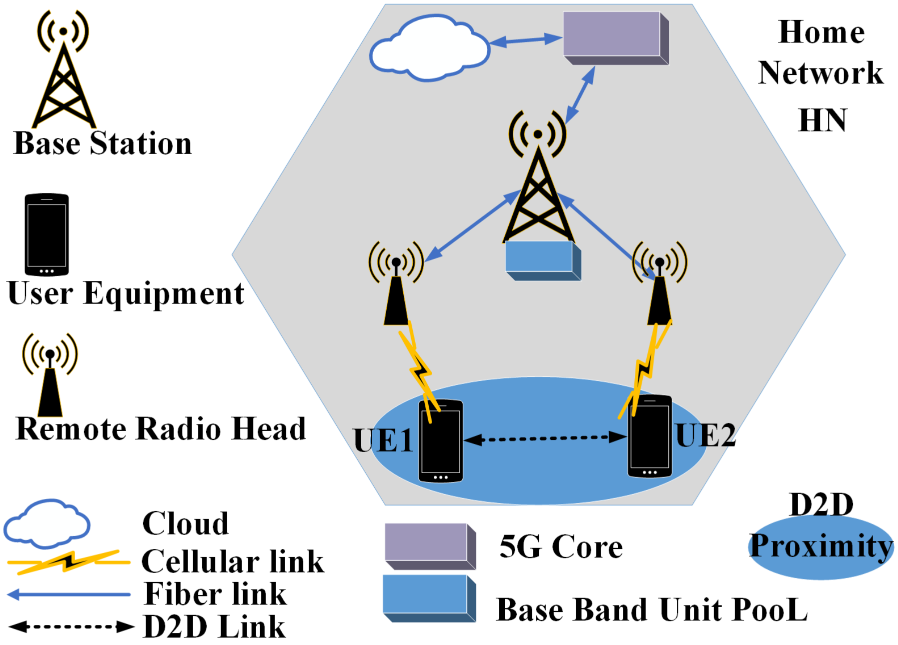

Fig. 1. 5G enabled D2D architecture.

The rest of the article is organized as follows. Section II presents an overview of NSD framework for 5G enabled D2D communications architecture, system, and service models. Security threats and threat model are discussed in section III. While in Section IV, X.805 framework is used to evaluate the security requirements of 5G enabled D2D communications. The existing security solutions and new approaches are discussed in section V. Finally, the article is concluded in section VI.

2 Network Service Delivery Framework

To investigate security of NSD, an access and delivery framework is presented in this section based on the network architecture in [16], NS abstraction in [20], and CCN architecture. It focuses on the entities' communication and how the services are accessed, cached and shared between UEs but not how the data is stored or accessed on the application level.

2.1 Network Architecture

Since D2D and ProSe functionalities for 5G are in process of being standardised, this article uses the D2D communications architecture in [20] as shown in Fig. 1 and presents an NSD framework that utilize on mobile content delivery and network functions. CCN is integrated with cellular network to enable content aware operations such as content resolution at edge which is within 3GPP standardization [14]. 5G Network Function Virtualization (NFV) [43] allows the sharing of infrastructure resources between Network Service providers (NSP) and the delivery of content to users through network slicing. D2D communications, content delivery and content sharing are classified as NSs. ICN in 5G can be implemented using NFV and Software Defined Network (SDN) where ICN based service delivery methods such as CCN inherently integrate into the network infrastructure [58].

5G adopts C-RAN architecture [16], which centralizes the baseband resources to a single virtualized Base Band Unit (BBU) pool, then connects to several radio transceiver units called the Remote Radio Heads (RRHs) [39]. It enables virtualization, facilitating network infrastructure sharing [42] and the interface between BBU and RRH has been changed from circuit fronthaul to packet fronthaul. BBU is divided into Distributed Unit (DU) which is responsible for physical layer as well as real time Media Access Control (MAC) layer process and Centralized Unit (CU) responsible for upper layer computations process [66]. In 5G, the UE connects to 5G core network (5GC) via the new generation Radio Access Network (ngRAN) then to other Network Functions (NF) such as Access and Mobility Function (AMF), Session Management Function (SMF), Authentication Server Function (AUSF), User Plane Function (UPF), and Unified Data Management (UDM) as defined in [3], illustrated in Fig. 2.

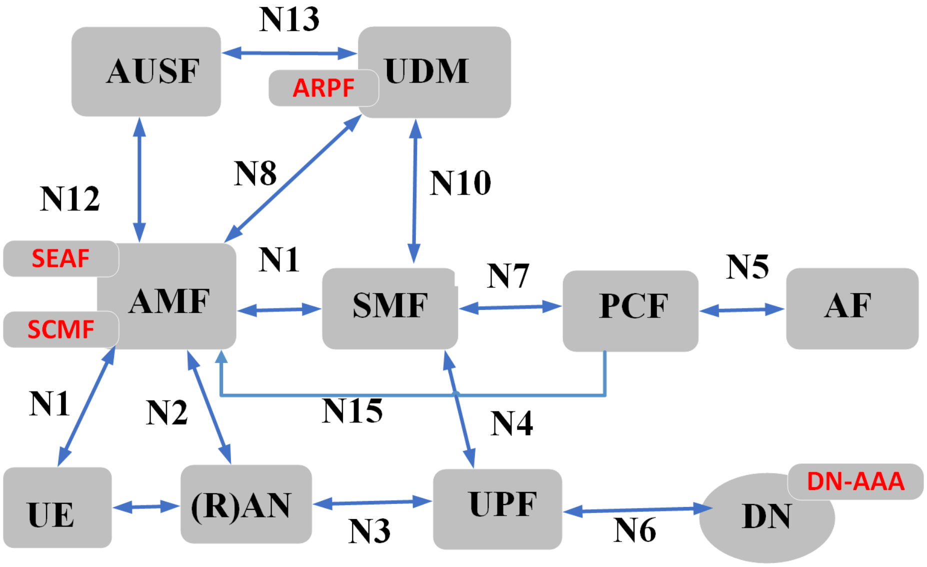

Fig. 2. 5G system architecture.

2.2 Security Architecture

The current security standards are not adequate for 5G, which affects new mission critical services and use cases. Therefore, there is a need for security architecture [4] that enforces trust between new actors and other entities in the HN [21]. The mobile network still consisted of three essential parties:

- UE: Consists of a Mobile Equipment (ME) and the Universal Subscriber Identity Module (USIM).
- Home Network (HN): It houses the user database and other security functions that stores users' subscription data and security credentials such as Subscription Permanent Identifier (SUPI) and the long-term key K.
- Serving Network (SN): The access network that the UE connects to via ngRAN.

The security architecture introduces new security entities such as Security Anchor Function (SEAF), AUSF, Authentication Credential Repository and Processing Function (ARPF) [4], [21]. The security architecture will have to consider NFV and SDN to achieve the objectives of 5G. Security enablers in 5G need to address key security concerns such as authentication, authorization, availability, privacy, trust, security monitoring, network management and virtualization isolation. Security Control Classes (SCC) are introduced to describe the security aspect of 5G system, SCC are mapped with security requirements based on X.805 eight security dimensions [73], [5].

2.3 System Model

The system model in Fig. 3 consists of following entities: UE, BBU pool, RRH, HN, and SN. The UE is registers to HN and receives the roaming services from Visiting Network (VN). The CCN protocol could be embedded into the UE, BBU pool, edge routers and 5GC [58] or control and user plane enhancement could be implemented to enable services like ICN within 5GC and extend the interfaces to support ICN Protocol Data Unit (PDU) sessions [59]. The UE will request to connect to the network, get authenticated then request to access the other services as per subscription agreements. To access these service other security procedures might be required [22], [21], [23].

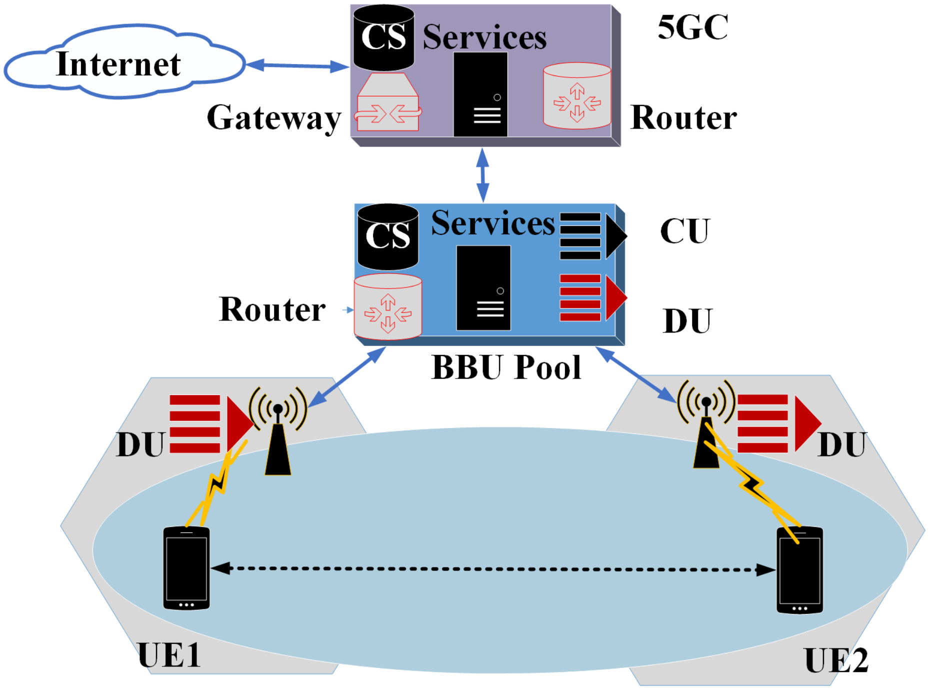

Fig. 3. System model.

Beside the usual management of cellular network and service operations, the MNO and SP will control internetwork service access and content retrieval to a certain extent. In 5G, the SP could be the MNO, third-party or another SP using the shared infrastructure as tenant provided by the MNO through network slicing. With MNO controlling service access and security management, it will be able hide its visibility or deny the UE from accessing a particular services. We more interested in content access and retrieval process part of D2D communication and discovery.

For data access and delivery, the UE requests for a content and interest message is forwarded to the BBU through RRH using the CCN forwarding process to full the UE request [58], [76]. The request could satisfied at by UE in proximity, Content Store (CS) in BBU Pool or in the 5GC CS. The CCN process involves local caching and satisfaction at different levels of the system model like the at edge as shown in Fig. 3. This enables offloading of the traffic from the backhaul to the edge if the request and data matching do not reach the 5GC. BBU also discovers cached content by associated devices and content transmission is performed through D2D communications [37]. However this process exposes the involved entities and data to various threats, hence the need for a comprehensive security requirements evaluation for the system model.

3 Security and Privacy for NSD in 5G Enabled D2D Communications

In this section, the threat model and threats that can affect the system model are presented. Security and privacy are serious concerns in 5G enabled D2D communications due to its characteristics. The UE's participation in content transmission, distribution, delivery and traffic offloading [33], not only increases its own exposure to threats but also of other entities and the data. Mobile security at edge is another concern, where the services and user's data will be most accessed. Also, communication channels between networks and D2D devices will be vulnerable to attacks, even the HN and VN might want to eavesdrop on D2D communications [68]. The MNO must authenticate and validate the SP to ensure legitimate access and provision of their services. In addition, the security context could be compromised and exposed outside the HN [5].

3.1 Threat Model

To evaluate security and privacy protection mechanisms for 5G enabled D2D communications, it requires a clear adversary. In this case , the threat model used is based on a Dolev - Yao (DY) model [19], an adversary model that formally models the attack against communication. DY is assumed to be the communication channel, capable of tapping the channel and eavesdrop on the transmitted messages. The DY can create, read, capture, replay and send messages on the wireless and wired communication channel in the network. In addition, the adversary can compromise UEs by revealing the secrets between UEs as well as applying her own public functions such as encryption and hashing. The adversary can impersonate any entity participating in the transaction, capable of initiating communication and responding to interest message sent by legitimate UEs. Might also try to repudiate their malicious behavior, preventing data sharing between UEs, hence denying service to other UEs and network entities.

3.2 Security Threats

Most studies have focussed on ICN integration with mobile network architecture, caching strategies [67], [15], [38]. Other studies have investigated security in ICN and D2D communications separately, while security issues in an integrated mobile network have not been investigated. The security and privacy in D2D communications were investigated in [68], [75], [34] however they did not use a systematic approach in their investigations. While the authors in [49] investigated the challenges in ICN based on NetInf architecture, evaluated the security requirements using the X.805 framework. They described the problems without the scope of the future challenges. In [65] a survey was conducted on ICN security but did not elaborate on the security challenges in heterogeneous networks such as next generation mobile network. While [7] conducted a survey on attacks affecting most ICN architectures but did not include attacks on CCN.

The wireless nature of D2D communications plus its characteristics and architecture present several security vulnerabilities that put network at risk to potential threats [1]. 5G can still be affected by the vulnerabilities from legacy systems and the security of NS might be compromised by new attacks on different levels of the network including the network slices. In cellular network, the BS acts as a Central Authority (CA) but in D2D communications it might play a minimal part hence strong anonymity is provided. However, the BS will have access to the data transmitted between the UE and other UEs, which could expose the data to possible attacks in form of active and passive, local and extended. We discuss some of these attacks below:

Eavesdropping: D2D messages can be eavesdropped by unauthorized users and authorized cellular users. In addition, side channel attacks across network slices targeting the implementation of cryptography or running a code to influence the contents of the cache [10].

Data Fabrication: The unprotected transmitted data can be fabricated or changed by malicious users, which leads to the content being circulated by unaware infected device to other devices such as modification of control data.

Impersonation Attack: A legitimate user might be impersonated by malicious user and communicate to other D2D users through identity impersonation and masquerading attacks. Also, network slice instance are vulnerable to these attack, which could lead to other attacks like monitoring or location attacks [10].

Free-Riding Attack: In D2D communications devices participate in sending and receiving data willingly but some UEs might not be willing to send data to others when in power saving mode while receiving data from its peers, which decreases the system availability.

Privacy Violation: It is important to protect the privacy of users' data such as their identity and location. If an attacker is able to listen and intercept transmitted messages and she would be able to extract information and guess the location of the UE. ICN cached content, user privacy and content names are all targets of privacy attacks. Moreover, user's subscription information could be leaked by a malicious attacker or compromised publisher through attacks such as timing, protocol and anonymity attacks [65].

Denial of Service (DoS) Attack: D2D services might be interrupted by making them unavailable to the intended users, by weakening or blocking legitimate devices from establishing connection completely. An attacker can send big continuous request to ICN nodes for services such as content, domain name queries or initiate interest flooding attack [6]. Also an attacker might exhaust security resources in one network slice so that she can attacker other slices [10].

Content Poisoning Attack: It involves filling the content router's cache with invalid content that ahs valid name matching the sent interest, however, the payload might be fake or with invalid signature [26].

Cache Pollution Attack: A malicious attacker may weaken caching activity by requesting less popular content frequently with attacks such as locality disruption and false locality [65].

Unauthorized access: An unauthorized node might access an object which was intended for a specific entity. For instance, in unauthorized cache access, a cached object from a local device might be access by unauthorized device [49].

Cache Misuse: The attacker can utilize on caches capability and use it as storage, hence, enabling the attacker to make her own content available. Also, an attacker can corrupt the cache content turning it into incorrect returned objects for DoS attack.

False Accusation: A malicious publisher tries to make it look like the requester has requested an object when it is not the case and might also charge a subscriber for services that was never requested or obtained.

IP Spoofing: Attackers uses malicious code to manipulate header of IP packets.

Location Spoofing: Attacker sends a fake location information to disturb D2D formation by imitating with artificial locations to confuse the D2D members.

Session Hijacking: The attacker spoofs the IP address of the victim device and guesses the sequence number expected by the targeted source device, this is followed by a Distributed DoS (DDoS) attack on the victim device, impersonate the device to carry on the session with the targeted device.

Communication Monitoring: The attacker with access to the same router as that requester is using to receive content then the attacker targets a requester and tries to identify the victim's requested contents.

Jamming Attack: Malicious user masquerading as legitimate subscriber sends many malicious content requests to disrupt the flow of information and replies are sent to a destination other than the requester's. In 5G jamming is achieved through analysing physical control link channels and signals [44].

Data Leakage: The UE might be attached to several slices on the network level with different security parameters. If the UE cannot separate data from different slices, the separation between slices could decrease, leading to the UE receiving sensitive data from one slice and then publish that data via another slice [10].

4 Security Evaluation of NSD in 5G Enabled D2D Communications using X.805 Framework

In this section, X.805 framework [73] is applied to evaluate the security requirements for delivering secure NS based on a system model, threat model and the NS abstraction in [20] which are mapped with X.805 security layers, planes and dimensions.

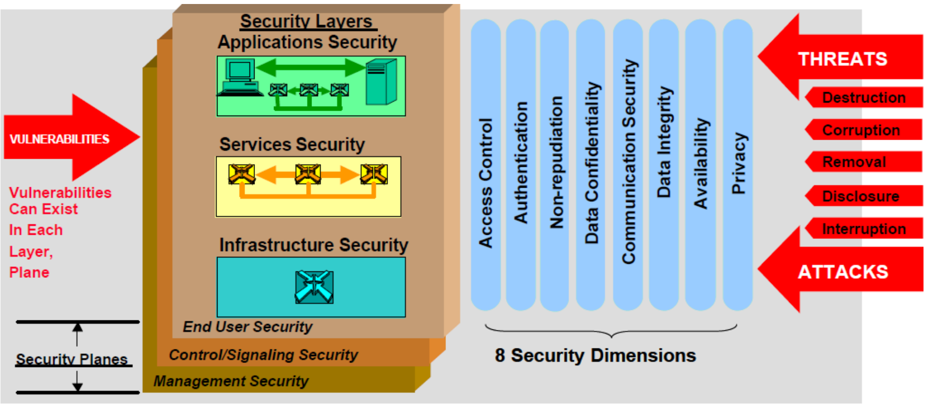

Fig. 4. X.805 security framework (Zeltsan, 2005)

4.1 The X.805 Security Framework Overview

Evaluating security in any networking system is very complicated, International Telecommunication Union Standardization Sector (ITU-T) developed X.805 framework as a security analysis tool. The X.805 framework uses a modular method to create a multi layered framework which assesses possible threats and vulnerabilities in end to end security to address security threats in networking systems effectively. The X.805 defines following: three security layers (applications, services and infrastructure); three security planes (end user, control and management; and eight security dimensions (access control, authentication, non- reputation, data confidentiality, communication security, data integrity, availability and privacy). The security layers and security planes are identified according to the network activities as illustrated in Fig. 4. In addition, nine security viewpoints are created by applying each security plane to each security layer, whereby each viewpoint has its own distinctive vulnerabilities and threats based on security dimensions.

Security Layers: The infrastructure security layer covers the fundamental building blocks of NS, NF, network slices, applications and individual communication links such as BS, RRH, routers, servers, slices and fibre links. This layer facilitates security of hosts involved in the data transmission, it prevents attacks from air interfaces and physical links including content servers, gateways, BBU and D2D connectivity. While service security layer covers services provided to end-users such as CCN, IP, cellular, QoS and location services. Securing this layer is complicated by the fact that services may build-upon one another to satisfy user requirements such as sharing and delivery of services via D2D communications. The CCN is related to the service layer while D2D communications is related to the infrastructure layer.

Security Planes: The security planes are concerned with securing the operations and provisioning of the individual mobile network elements, communication link as well as securing the functions of NS such as the configuration of UE, BBU, 5GC and secure content provisioning. In addition, its concerned with securing the control data in the network elements and in transit for NS such as D2D control link and PDU session. It ensures the security of the end user data on the network elements.

Table 1. Infrastructure Layer in Relations with Security Dimensions.

Security Dimensions	**Infrastructure Layer**	**Security Mechanisms**
Access Control	Authorize UE and network entities to accessing data on the UE and other entities	ACL, passwords
Authentication	Verify the identity of the UE, BBU and server providing the NS to the UE	Shared secret, PKI digital signature, digital certificate
Non-repudiation	Record UE, BBU, servers that perform activities on devices while accessing the NS	MAC, hash , function encryption
Data confidentiality	Protect the data on network devices, on UE and and control data	Symmetric and asymmetric encryption
Communication security	Ensures that UE, control and management data is only transmitted on sure channels	Symmetric and asymmetric encryption
Data integrity	Protect data on network entities, in transit and control data against unauthorized modification	MAC, hash function, digital signature
Availability	Ensure that network devices can receive and access UE data and manage D2D links	IDS,IPS, BC, DR
Privacy	Ensure that data which can identify the entities is not available to an unauthorized users	Encryption

Security Dimensions: The eight security dimensions are used as a viewpoint for vulnerabilities and threats to provide protection against any attack in form security controls such as the authentication, availability, integrity, confidentiality, and access control on each layer.

Table 2. Service Layer in Relations with Security Dimensions.

Security Dimensions	**Service Layer**	**Security Mechanisms**
Access Control	Authorize BBU and SP to perform management activities on NSs	ACL, passwords
Authentication	Verify the identity of the NSs, the service entities on the and the origin of the NS	Shared secret, PKI, digital signature digital certificate
Non-repudiation	Record the SP, UE, BBU to prevent deny the transactions and origin of the control message	MAC, hash function encryption
Data confidentiality	Protect the NS's data transiting the network devices from unauthorized access	Encryption and
Communication security	Ensures that NS management, control data for UE passes through a secure channel	Encryption
Data integrity	Protect the management, control, the UE data against unauthorized modification and deletion	MAC, hash function, digital signature
Availability	Ensure that the network devices UE data and D2D link available to receive control data	IDS,IPS, BC, DR
Privacy	Ensure that data that can be used to identify NS is not available to unauthorized users	Encryption

4.2 Security Evaluation using X.805 Framework

To able to mitigate these potential threats against the system model, the security requirements must be evaluated. This article focusses on the service and infrastructure layers of the system. It classifies security requirements using security layers, associated with the security planes in modular format, each module is analysed using the eight security dimensions, summarised in Tables 1 and 2. The modules 1, 2 and 3 are based on infrastructure layer whereas modules 4, 5 and 6 are associated with service layer. The X.805 demonstrates a methodical approach in tabular form as shown in Fig. 5 and Fig. 6, the security objectives of the dimensions for each module are analysed. The security goal is to cover the security capability of the framework including the detection and recognition of attacks, protection of the system, audit of the system and its recovery after the attack. Based on the above potential threats, the NS using infrastructure of cellular network should meet the certain security requirements. A comprehensive security analysis follows in the next subsections.

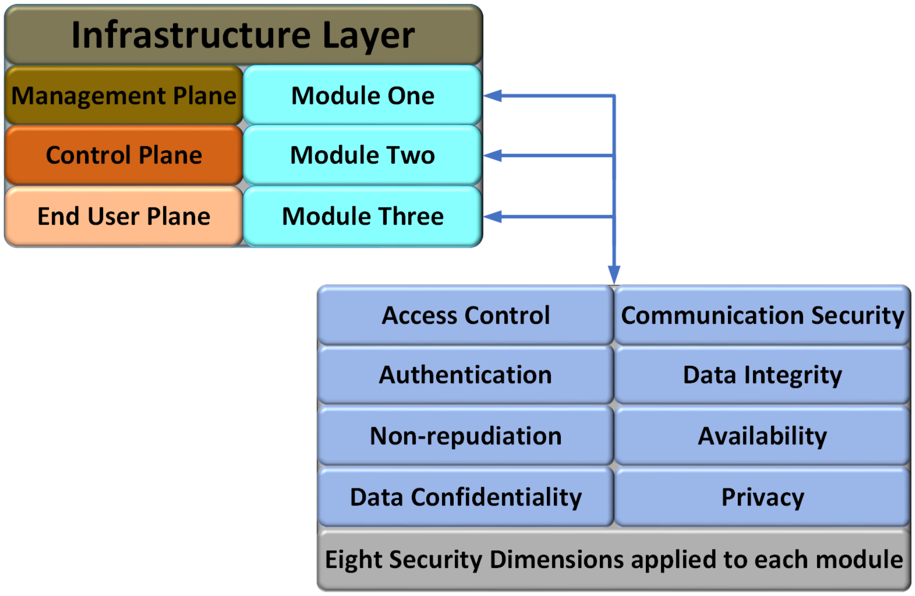

Fig. 5. Infrastructure Layer with Eight Dimensions.

Access Control This dimension limits and control access to network elements and services through Access Control (ACL), encryption and authorization mechanisms. Some services lack a built in support to provide ACL or authorization framework. When an entity that is not controlled by the SP publishes content, the SP has no way of applying access control or knowing which user has accessed or cached data [53]. In addition, the system should be able to revoke user's privilege if it is detected to be a malicious user. Attacks such as free riding should be prevented and UE should be protected from joining rouge BS. Also, privileges of D2D users should be deprived in time if a user is found out to be malicious or their subscription has expired and revocability can prevent impersonation attack.

Infrastructure Security Layer - *Modules 1, 2 and 3*: The ACL at this layer is concerned with only allowing authorized UE and network entities to perform activities such as accessing data on the UE and in the network. Without the appropriate ACL policies, an unauthorized device might be able to access

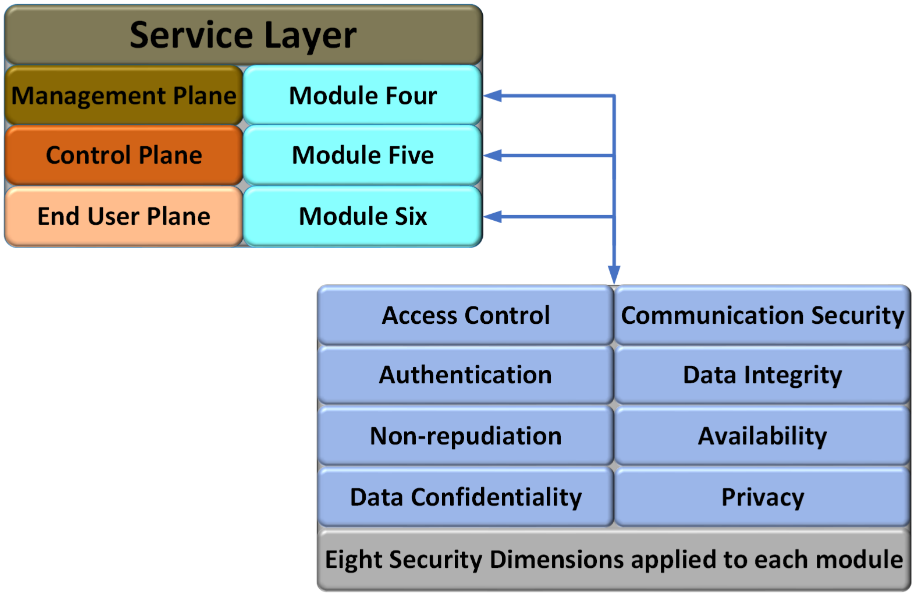

Fig. 6. Service Layer with Eight Dimensions.

services which were intended for limited UEs. ACL can permit or deny the SP and a device the right to perform any action on service or device during the D2D communications. Therefore, extra mechanisms should be in place for the UE to control the data flow. ACL must be applied to control the access of data and activities on the network entities.

Service Security Layer - *Modules 4, 5 and 6*: The ACL at this layer is concerned with allowing only authorized BBU and SP to perform management activities on the NS and that the received service originated from authorized source. In addition, it only allows authorized UE to access the NS and to ensure the request message originated from an authorized UE before being accepting. The BBU should be able hide its services or visibility from the unauthorized UE after the authentication and during handover session. ACL mechanisms such as Role-Based Access Control (RBAC) or Discretionary Access Control (DAC) must be applied on the service entities and should depend on the identity of the subject for authorization, it suits unstructured domains like the system model in this article.

Authentication This dimension ensures a valid proof of identity is presented in form of shared secret, Public Key Infrastructure (PKI), digital certificate [8]. Authentication evaluates the identity of a party and verifies if the party is in possession of a secret and a key, it can be applied on an entity and data. Assigning an identity to a secret or key is required during authentication. For the UE to access the NS, the UE and network must perform authentication using

Authentication and Key Agreement (AKA) methods [4]. In 5G, after a successful primary authentication, a secondary authentication can be performed to ensure that only authorized UEs can access SP services. UEs, service and the network must be able to mutually authenticate to stop attacks such as impersonation attack, false content injection and free riding.

Infrastructure Security Layer - *Modules 1, 2 and 3*: Authentication at this layer is concerned with verifying the identity of the UE requesting the services, SN, BBU and service entities providing the NS to the UE. The identity of the entities and transmitted data must be authenticated to secure D2D communications. The first step is to authenticate the entities to confirm the D2D peers' identities then authenticate data sources to confirm if it is from legitimate users [75]. Also, authentication can be achieved when the requester verifies signature that was used to digitally sign the data by the publisher. If UE A receives a message from UE B, A can verify that B is indeed the sender of the message where A and B can be any of the device in the network such as UE, server, which can also be classified as subscribers and MNO/SP [49].

Service Security Layer - *Modules 4, 5 and 6*: The authentication on this layer is concerned with verifying the identity of services and the origin of the NS. The verification of UE trying to access the services should be done by Authentication, Authorization and Accounting servers (3As), which also monitor, manage the subscription and service provisioned for the UE. The service should also be able to verify the authenticity of the UE. The receiver should be able to assess the validity, provenance and relevance of the data received [53], to make sure that fragmented data received is complete and not corrupted. Therefore, verifying the producer's identification to ensure that identity and source of cached data can be trusted [8] is a must.

Non-Repudiation This dimension is concerned with preventing any device from denying its involvement in an activity on the network such as denying transmitting or receiving a service [75]. It also allows the tracking of the source of a possible security violation. The SP and devices should be held accountable for their action through monitoring of network activities [49]. For example, a verified content producer should not be able to deny that they are the source of the content or UE should not be able to deny sending an interest message. Some of the solutions include the use of digital signature to achieve non-repudiation and other mechanisms should be in place to prove originality of the data as well as proof of transaction to prevent attacks such as false accusation.

Infrastructure Security Layer - *Modules 1, 2, and 3*: The non-repudiation at this layer records and identifies entities such as UE, BBU, servers that perform activities on other devices, modify control data or access UE data. This record can be used as proof of access or modification of the control data. In additional, identifies the origin of control messages and the action that was performed. Identifiers can be applied as solution to bind user related messages to the UE and network for accountability. Also, Packet Level Authentication (PLA) protocol

[11] can be used to provide network layer authentication and accountability of the data using public key cryptography.

Service Security Layer - *modules 4, 5 and 6*: The non-repudiation at this layer is concerned with recording the content producer, UE, BBU or other entities that performed activities on the NS, origin of the control message and the UE that accessed the services. For example, recording information about an object's provenance, indicating the creator or publisher of content object. Moreover, the requester who receives content can be recorded and charged for the service using out-of-band digital signature solution [50]. There should be a strong association between the entity identities and use of the NS to prevent attacks like spoofing attack. However due to the nature of integrated system there might not be a direct link between SP and the requester. Therefore, the producer and requester must trust the system to account for usage in a fair manner, whereby charges are added according to services accessed periodically [9]. Traditionally, the mobile network is capable of tracking and monitoring the system utilization and usage as per the contract between the SP and the subscriber.

Data Confidentiality This dimension ensures the confidentiality of data on the UE, network devices and in transit, encryption should be used on data to provide confidentiality. Encrypted data and should only be decrypted by the authenticated and authorized entity. The confidentiality of any used data must be protected against unauthorized users or attacks such as eavesdropping and privacy invasion. Moreover, encrypting message on wireless channel will be standardized in 5G. For example, encryption keys can be applied to encrypt data using symmetric or asymmetric encryption mechanisms.

Infrastructure Security Layer - *Module 1, 2 and 3*: The data confidentiality at this layer is concerned with protecting data on the network devices and data transiting in transit from unauthorized access such as user's control and configuration data. During service provision, data might pass through possibly untrusted segments, which highlights the issues of whether the producer and requester are able to trust the infrastructure routing decisions without exposing the data. Encryption and ACL mechanisms can be used in providing data confidentiality. Other methods such as key extraction protocol based on Channel State Information (CSI) could be used to avoid leakage of data. Additional use of cryptographic mechanism like stream ciphers, might stop the attacker from reading messages between D2D users as well as preventing eavesdropping attack [34].

Service Security Layer - *Module 4, 5 and 6*: Confidentiality at this layer is concerned with protecting the NS's control, configuration and management data such as Pending Interest Table (PIT) updates, security setting from unauthorized access and modification. ACL and encryption methods can be used to provide confidentiality of NS. A content producer should be able to control which subscribers may receive what content, however confidentiality might not be relevant where the producer is offering data to everyone. Group key distribution [48] is another mechanism that can be used for data confidentiality, the producer pre-distributes keys to all potential requesters, an out-of-band approach prearrangements might be required [49].

Communication Security This dimension ensures that information only flows from source to destination endpoints using secure wireless and wired communication channels. The end user accesses resources and services by connecting to the network via wireless access point. In legacy systems, the wireless channel was not secured but in 5G this problem will be addressed [4]. However, point-to-point communication does not apply to ICN, the content is requested without being aware of its location. Also, the requester might be receiving different chunks of cached data from different sources such as content server, BBU Pool and D2D UEs which makes establishing secure connections complex and unmanageable. Therefore, information-centric and host-centric security methods must be considered, it is paramount to ensure that only intended D2D users are able to receive and read data. Encryption methods can be used to provide confidentiality, secure routing and transmission of data to authorized users. With D2D communications, physical layer security can be applied by exploiting wireless channel characteristics, modulation, coding, and multiple antennas preventing eavesdroppers [64].

Infrastructure Security Layer - *Modules 1, 2 and 3*: The communication security at this layer ensures that UE, control and management data only flows between entities and communication link that uses secure channels. For example, authentication data such as security context should not be diverted or intercepted as it flows between source and intended destination end points. Secure communication must be established between the UEs and other entities before sharing any information.

Service Security Layer - *Modules 4, 5 and 6*: The communication security at this layer ensures the management, control and UE data in transit for use by NS, only flows between entities using a secure channel and that data is not intercepted as it flows between the endpoints. For example, with the interest messages and service data, the SP registers a service identity to the server or cache node and binds the data under namespace. The BBU is tasked with monitoring and storing data regarding the interest and data exchange, BBU can search for malicious nodes and select alternatives path for packets to reach their destination securely, taking advantage of the ICN architecture which can reveal misbehaving nodes [56].

Data Integrity This dimension ensures that data is received as sent or retrieved as stored and no data manipulation has been performed by any malicious or authorized users. D2D users should be able to receives correct data without alteration or fabrication. If an attack like message injection or false reporting are initiated, the data's integrity might be violated which could compromise the UE and the whole system [45]. Data integrity can be achieved by using hash, functions, MD5, digital signature, while integrity in CCN can be provided by applying a simple content-signing method, such as the manifest-based content authentication.

Infrastructure Security Layer - *Module 1, 2 and 3*: The integrity at this layer is concerned with protecting the configuration, control data on the network entities, D2D links and data in transit or stored on the devices against unauthorized modification, creation and replication. System integrity can be compromised if an attacker uses a malicious server to insert bogus subscription and act as a bogus subscriber to the UE or BBU, then responds to interest with bogus reply or drop the data completely. Integrity is important for D2D communications to secure the user's data and enable legitimate users to decrypt the received encrypted data by using encryption.

Service Security Layer - *Module 4, 5 and 6*: The integrity at this layer is concerned with protecting the management, control, UE data against unauthorized modification, and deletion of service data. For example, the integrity of interest and service data in transits should be protected. The identifications and security context from authentication should be protected from any modification or deletion [75]. Integrity can be ensured by applying cryptographic mechanisms such as hash functions, Message Authentication Code (MAC) and data modification should be detectable, however there is no cryptographic integrity protection for the user data plane in 5G.

Availability This dimension ensures network elements and services are available to legitimate and authorized users ubiquitously. Services should be available even during attacks such as DoS and free riding [75]. In D2D communications, DoS attacks are hard to detect since the D2D does not rely on centralized infrastructure [35]. Jamming attack affects communication between D2D users and can be started anonymously [34] affecting service availability. Due to CCN naturally spreading contents to permit request being satisfied by alternating sources, it requires a lot effort to initiate a DoS attack whereby an attacker would have to send repeated requests on a single device, it is hard but possible [49]. In 5G, NS should always be available for UEs and the waiting time to connect or get services should be as short as possible to complement 5G objectives like high date rate, ultra low latency and reliability. In addition, devices such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and firewalls should be deployed in the network as well as Business continuity (BC) and Disaster Recovery (DR) plans should in place to decrease downtime of 5G services.

Infrastructure Security Layer - *Module 1, 2 and 3*: The availability on this layer is concern with ensuring that network devices can receive control data, access UE data and manage the D2D link. Authorized UEs and other devices should have access to the infrastructure and protection against any attacks. During DoS attack, the attacker can target caching and routing plane by creating large amounts of unwanted traffic, which is cached by intermediate devices in the BBU and 5GC, resulting into cache overflow after overload of caching plane. Moreover, cache DoS attack can be initiated by polluting the content cache in CS, hence returning an incorrect content object [24]. To minimize the damage from such attack, no data should be delivered to any requests unless there is a valid subscription from the requester. Therefore, the prevention of unwanted traffic from bogus requests can improve availability and dependability whereby the system only serves valid and authorized users.

Service Security Layer - *Modules 4, 5 and 6*: The availability at this layer is concerned with ensuring that the NS are always available and accessing or managing of the NS by authorized users cannot be denied. Services must be protected from attacks such as DoS and jamming attacks. Whereby the attacker can use malicious content and subscriptions to overload the system, subscribers flood producer with bogus interest messages. Availability of services guarantees that authorized users can access the services through D2D communications. Availability and dependability can maintain satisfactory user experience.

Privacy This dimension ensures that the identifiers, user and network data is kept private. Privacy in 5G is part of a very critical security requirements, identity and location must be preserved. Privacy drives the new age of information and users data privacy has become a very sensitive topic, even though privacy in CCN architecture has not been investigated extensively but it has been in D2D communications. D2D users must be aware of which data they are sharing, and the system should collect only the required data to provide a specific service. Encryption can be used to the protect the communication and data transmission between entities.

Infrastructure Security Layer - *Module 1, 2 and 3*: The privacy at this layer is concerned with ensuring that data that can be used to identify the UE, BBU and 5GC entities or communications link is not available to unauthorized users. Network elements should not be able provide data revealing the UE's network activities such as UE's location to unauthorized user and only certain user data should be accessed by authorized personnel. Exposing information from cached data, the attacker could extract it hence violating user data privacy. The UE might need to communicate anonymously while accessing services to reduce such attacks [32].

Service Security Layer - *Module 4, 5 and 6*: The privacy at this layer is concerned with ensuring that data that can be used to identify devices, NS management systems, communication links is not available to unauthorized user. In addition, NS should not be able to reveal UE data such as UE and service identities. An attacker might be able to obtain data by monitoring cache transaction of accessed data even when the requester source is not clearly identified, this is achieved by analysing direction of the requests and timings of the transactions [49]. Location-based services can enable the tracking of the UE and data privacy might be compromised as this service relies on location of the user and service. Moreover, the UE activities can be exposed to cache owners that they might have no transactions with the UE. It is impossible for the user to request services without revealing their subscription and security information to the SP or the infrastructure. Private Information Retrieval (PIR) mechanism [71] could be used to preserve privacy of subscription data, it allows the retrieval of database entries without the user disclosing the entries to the server.

5 Security Solution Approaches

For solution approaches, we have to consider the unique characteristics of the CCN and 5G enabled D2D communications and how some of their security features are pre-designed. For instance, ICN has basic security in its architecture design such as integrity and authentication while the encryption messages over wireless communication has been standardised in 5G. In addition, the 5G trust enhancement is due to routing attacks in SS7 [25] impersonation and address spoofing attacks [61] in signalling messages which exploited the trusted domains in legacy systems. This section discusses possible security solutions to address the threats and attacks presented in this article.

5.1 Authentication and Key Management (AKM)

Authentication is a key factor in securing D2D communications, content delivery and facilitating content authenticity. A secure framework for authentication between two D2D users was proposed in [62] and [74] proposed a security communication protocol to defend systems from attacks like Man In The Middle (MITM) and masquerading. Data origin authentication method can be achieved by using of digital signature algorithm for proof of origin and protecting sensitive message from tampering. In addition, cryptography can be deployed at the different layers to achieve authentication. In this case, keys are used to encrypt and decrypt data, therefore key management plays a vital role in preservation of user and security context data. This includes the generation, distribution and storage of keys.

5.2 Confidentiality and Integrity (CI)

Data confidentiality of NS, D2D messages, control data can be implemented by using ACLs and various cryptographic techniques. While data integrity can be protected by using hash functions and digital signatures during transmission, preventing a malicious user from forging data that can affect the system's integrity. For instance, routing misuse is the result of concept of trustworthiness and integrity in CCN based on a trusted computing approach [12].

5.3 Non-Repudiation Enforcement (NRE)

The use of digital signature and certificates can act as proof of work so that entities don't deny their involvement in a transaction. When the UE registers for services, the SP can monitor the services accessed and bill the subscriber accordingly. An efficient auditing system can be used to stop attack such as false accusation by logging all activities in the network with platforms such as

Distributed Audit Service platforms (XDAS) [29]. The system should be able to identify the origin of false message through traceability. Additionally, the message originator can be verified through authentication process to avoid data leakage by false notifications from a malicious user.

5.4 Secure Naming, Routing, Forwarding and Transmission (SNRFT)

Content naming technique is fundamental to ICN, a verifiable binding between a content name and its provider prevents content poisoning attack. Methods such as secure naming, secure routing and forwarding techniques are vital to any network architecture security. Secure naming scheme can be achieved by using RSA and Identity Base Cryptography (IBC). A name-based method using IBC was proposed in [77] for trust management in CCN. While secure routing is essential in D2D communications especially during out of coverage, in [54] a Secure Message Delivery (SMD) protocol that protects relayed message was proposed. Whereas secure forwarding involves secure forward plane or secure namespace mapping that enable interest forwarding for name prefixes. The Interest Key Binding (IKB) method can be applied by binding the producer's public key and the content name with the interest packet [27], which maps the producer and the content.

5.5 Access Control (ACL)

Authorization enables an entity to control the access to its services requested by other entities. In mobile network, ACL can be enforced through use of RADIUS [46] and DIAMETER [13] protocols which are centralized authorization or through a distributed authorization method as proposed in [70]. Some of these ACL methods are encryption-based, attribute-based, session-based, Fine Grained Access Control (FAC) and context aware schemes. ACL can be supported by AKM to provide different levels of authorization such as access to the network and services. The authors in [72] focused on the D2D communications access, authorization was achieved by using heterogeneous and fine-grained access control mechanisms together with AKA methods. An identity-based cryptography for ACL enforcement was used in [60] while the authors in [52], proposed an ACL method for CCN based on Kerberos in IP-based networks, utilizing on distinctive authentication and authorization techniques.

5.6 Privacy Preservation (PP)

Integrating services in mobile network requires the UEs to disclose their location to the BBU for data routing and forwarding but UEs might be unwilling to share their location to avoid exposure. Privacy can be preserved by using identity expiration enforcement technique and leveraging on homomorphic cryptography [18]. The authors in [51] proposed a client anonymity framework, cryptographic based on naming scheme, it improves publisher's and consumer's privacy and untraceability. Also data privacy can be achieved through data encryption and physical layer security to define secrecy capacity as maximum transmission rate at which unintended user cannot decode transmitted message [40]. The obfuscation method is another way to preserve data privacy by degrading the quality of information like UE location to protect the user's identity.

5.7 Availability and Dependability (AD)

This approach is for both the D2D communications and services functionalities to reduce the defect attacks such as DoS and free riding that make services unavailable to legitimate users. An attacker can decrease system availability by encouraging UEs to selfishly not participate in content sharing, a cooperative mechanism between UEs was proposed in [63]. In CCN, DoS mitigation may include change in intermediate cache structure such as PIT and CS, as well as reducing the rate of consumer request through request of proof work [65]. Additionally, an interest flooding detection and mitigation method based on fuzzy logic and routers cooperation can be applied [69].

Table 3. Threats, Attacks and Solutions based on X.805 Framework.

Threats	Attacks	Solutions
Destruction of data and resources	Impersonation, MITM, routing misuse	CI, AKM
Corruption or modification of data	Content poisoning, false accusation, cache misuse, data fabrication, replay, IP/location spoofing	NRE, SNRFT
Theft, removal or loss of data resources	Unauthorized, access masquerading, false content injection, data leakage	AKM, ACL
Disclosure of data	Privacy violation, eavesdropping discovery, monitoring, timing anonymity, unlinkability, traceability	PP, AKM
Interruption of services	Cache pollution, DoS, free riding jamming, session hijacking interest flooding	AD, AKM

The presented solutions could be applied to multi layers of the network, based on the eight dimensions of X.805 framework using a modular based approach to address the vulnerabilities, threats and attacks. Also, Unconventional techniques such as cache verification and self-certifying naming methods can be applied to prevent forged content. Self-certifying is becoming a popular approach in 5G, to support network edge services, this is due its ability to handle dynamic content objects. Security on physical layer enforce security on the upper layers in D2D communications and it is necessary to study security on the high layers rather than just the physical layer. Moreover, security at upper layers is based on building security protocols to provide secure communication and data in transit without undermining D2D communications and 5G features such as network routing, caching or D2D links. Therefore, we believe the security threats in 5G require an integrated solution, hence a hybrid approach that consists of information-centric and communication-centric solutions should be used.

Many security issues in D2D communications and other NS are still open without appropriate solutions, some of the threats, attacks and possible solutions are presented in Table 3. No work is comprehensive enough to cover all security domains and fulfil all security requirements of 5G. Some of the existing work proposed solutions that achieve mobile security with IP based methods but not compatible with new use cases and services like CCN. Moreover, the security mechanisms should be lightweight to avoid high communication and computational overhead and the effects of mobility on security and privacy preservation should be considered.

6 Conclusion and Future Work

In 5G, D2D communications will be used as underlay technology to offload traffic from the backhaul to the fronthaul and push content to edge closer to the user. The secure delivery of NS to D2D users is crucial for 5G's main objectives. Due to heterogeneous nature of 5G and its enablement of new use cases, new security challenges have been created, making the secure delivery of NS difficult. Therefore, these new and old challenges need to be address using new and more robust measures. We investigated related work on the security of NS in 5G enabled D2D communications, our contribution included the introduction of NSD framework based on D2D and CCN as NS. We presented an integrated system model to investigate the security for both D2D and CCN domains, highlighting the vulnerabilities, threats, and attacks and their affect on D2D users. We then evaluated the security requirements of the system model based on X.805 security framework for a systematic and comprehensive approach. We also explored the existing approaches, then suggested a hybrid approach consisting of information-centric and host-centric solutions to provide security for hosts, the data, and the network. Most importantly, the study highlighted the lack of an integrated approach to address security for NSD in 5G enabled D2D communications which needs addressing. The open issues will motivate future research trends including security for SDN/NFV, network slicing, and integrated security solutions for 5G. Therefore, future work is to develop a comprehensive multi-layered security framework and solutions that addresses the highlighted security issues by incorporating the possible solution approaches in this article.

References

1. 3GPP: Feasibility study on the security aspects of remote provisioning, change of subscription for machine to machine (m2m) equipment. Technical specification

(TS) 3GPP TR 33.812 V9.2.0 (2010-06), Third Generation Partnership Project (2010)

2. 3GPP: Feasibility study for proximity services (prose). Technical specification (TS) 3GPP TR 22.803 V12.2.0 (2013-06), Third Generation Partnership Project (2013)
3. 3GPP: Study on architecture for next generation system. Technical specification (TS) 3GPP TR 23.799 V14.0.0 (2016-12), Third Generation Partnership Project (2016)
4. 3GPP: Proximity-based services (prose); security aspects. Technical specification (TS) 3GPP TS 33.303 V16.0.0(2020-07), Third Generation Partnership Project (2020)
5. 5GPPP: Deliverable d2.7 security architecture (final). Tech. rep., 5G Enablers for Network (2017)
6. Aamir, M., Zaidi, S.M.A.: Denial-of-service in content centric (named data) networking: a tutorial and state-of-the-art survey. Security and Communication Networks **8**(11), 2037–2059 (2015). https://doi.org/10.1002/sec.1149
7. AbdAllah, E.G., Hassanein, H.S., Zulkernine, M.: A survey of security attacks in information-centric networking. IEEE Communications Surveys & Tutorials **17**(3), 1441–1454 (2015). https://doi.org/10.1109/COMST.2015.2392629
8. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., Ohlman, B.: A survey of information-centric networking. IEEE Communications Magazine **50**(7), 26–36 (2012). https://doi.org/10.1109/MCOM.2012.6231276
9. Aiash, M., Mapp, G., Lasebae, A., Loo, J.: A secure framework for communications in heterogeneous networks. In: 2014 28th International Conference on Advanced Information Networking and Applications Workshops. pp. 841–846. IEEE (2014). https://doi.org/10.1109/WAINA.2014.132
10. Alliance, N.: 5g security recommendations package 2: Network slicing. White paper (2016)
11. Andersen, D.G., Balakrishnan, H., Feamster, N., Koponen, T., Moon, D., Shenker, S.: Holding the internet accountable. In: HotNets. Citeseer (2007), http://repository.cmu.edu/compsci/66. (Accessed 16 January 2021)
12. Anderson, R.: Cryptography and competition policy issues with "trusted computing". Computer Security Journal **20**(1), 1–13 (2004)
13. Arkko, J., Zorn, G., Fajardo, V., Loughney, J.: Diameter base protocol. Rfc, IETF (2012), https://tools.ietf.org/html/rfc6733. (Accessed 10 January 2021)
14. Carofiglio, G., Gallo, M., Muscariello, L., Perino, D.: Scalable mobile backhauling via information-centric networking. In: The 21st IEEE International Workshop on Local and Metropolitan Area Networks. vol. 2015-, pp. 1–6. IEEE (2015). https://doi.org/10.1109/LANMAN.2015.7114719
15. Chandrasekaran, G., Wang, N., Hassanpour, M., Xu, M., Tafazolli, R.: Mobility as a service (maas): A d2d-based information centric network architecture for edge-controlled content distribution. IEEE Access **6**, 2110–2129 (2018). https://doi.org/10.1109/ACCESS.2017.2781736
16. Checko, A., Christiansen, H., Yan, Y., Scolari, L., Kardaras, G., Berger, M., Dittmann, L.: Cloud ran for mobile networks-a technology overview. IEEE Communications Surveys & Tutorials **17**(1), 405–426 (2015). https://doi.org/10.1109/COMST.2014.2355255
17. Cisco: Cisco visual networking index: Global mobile data traffic forecast update, 2016–2021 white paper. Tech. rep., Cisco (2017), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html. (Accessed 09 September 2018)

18. Dijk, M.V., Gentry, C., Halevi, S., Vaikuntanathan, V., Gilbert, H.: Fully homomorphic encryption over the integers. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. vol. 6110, pp. 24–43. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_2
19. Dolev, D., Yao, A.C.C.: On the security of public key protocols. IEEE Transactions on Information Theory **30**(2), 198–208 (1983)
20. Edris, E.K.K., Aiash, M., Loo, J.: Investigating network services abstraction in 5g enabled device-to-device (d2d) communications. In: 2019 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). pp. 1660–1665. IEEE, Leicester, UK (Aug 2019). https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00296
21. Edris, E.K.K., Aiash, M., Loo, J.: Formal verification and analysis of primary authentication based on 5g-aka protocol. In: The Third International Symposium on 5G Emerging Technologies (5GET 2020). IEEE, Paris, France (Jun 2020)
22. Edris, E.K.K., Aiash, M., Loo, J.: Network service federated identity (ns-fid) protocol for service authorization in 5g network. In: 5th IEEE International Conference on Fog and Mobile Edge Computing (FMEC 2020). IEEE, Paris, France (Jun 2020)
23. Edris, E.K.K., Aiash, M., Loo, J., Alhakeem, M.S.: Formal verification of secondary authentication protocol for 5g secondary authentication. International Journal of Security and Networks (accepted for publication)
24. Edwall, T.: The network of information: Architecture and applications. Tech. rep., SAIL Project Team (2011), https://sail-project.eu/wp-content/uploads/2011/08/SAIL_DB1_v1_0_final-Public.pdf. (Accessed 02 June 2019)
25. Engel, T.: Ss7: Locate. track. manipulate. In: Talk at 31st Chaos Communication Congress (2014)
26. Ghali, C., Tsudik, G., Uzun, E.: Elements of trust in named-data networking. ACM SIGCOMM Computer Communication Review **v44**, 12–19 (2014). https://doi.org/10.1145/2677046.2677049
27. Ghali, C., Tsudik, G., Uzun, E.: Needle in a haystack: Mitigating content poisoning in named-data networking. In: NDSS Symposium (2014). https://doi.org/10.14722/sent.2014.23014
28. Golrezaei, N., Molisch, A.F., Dimakis, A.G., Caire, G.: Femtocaching and device-to-device collaboration: A new architecture for wireless video distribution. Communications Magazine, IEEE **51**(4), 142–149 (2013). https://doi.org/10.1109/MCOM.2013.6495773
29. Group, O.: Distributed audit service (xdas) (1998), http://www.opengroup.org/security/das/xdas_int.htm. (Accessed 05 June 2019)
30. Guey, J.C., Liao, P.K., Chen, Y.S., Hsu, A., Hwang, C.H., Lin, G.: On 5g radio access architecture and technology [industry perspectives]. Wireless Communications, IEEE **22**(5), 2–5 (2015). https://doi.org/10.1109/MWC.2015.7306369
31. Gupta, A., Jha, R.K.: A survey of 5g network: Architecture and emerging technologies. IEEE Access **3**, 1206–1232 (2015). https://doi.org/10.1109/ACCESS.2015.2461602
32. Hamoud, O.N., Kenaza, T., Challal, Y.: Security in device-to-device communications: a survey. IET Networks **7**(1), 14–22 (2018). https://doi.org/10.1049/iet-net.2017.0119

33. Han, B., Hui, P., Kumar, V.A., Marathe, M.V., Pei, G., Srinivasan, A.: Cellular traffic offloading through opportunistic communications: a case study. In: Proceedings of the 5th ACM workshop on Challenged networks. pp. 31–38 (2010). https://doi.org/10.1145/1859934.1859943
34. Haus, M., Waqas, M., Ding, A.Y., Li, Y., Tarkoma, S., Ott, J.: Security and privacy in device-to-device (d2d) communication: A review. IEEE Communications Surveys & Tutorials **19**(2), 1054–1079 (2017). https://doi.org/10.1109/COMST.2017.2649687
35. Huang, H., Ahmed, N., Karthik, P.: On a new type of denial of service attack in wireless networks: The distributed jammer network. IEEE Transactions on Wireless Communications **10**(7), 2316–2324 (2011). https://doi.org/10.1109/TWC.2011.052311.101613
36. Jacobson, V.: A description of content-centric networking (ccn). Future Internet Summer School (FISS) **2018**(Nov 28,) (2009), https://named-data.net/publications/van-ccn-bremen-description/. (Accessed 10 March 2021)
37. Jin, H., Xu, D., Zhao, C., Liang, D.: Information-centric mobile caching network frameworks and caching optimization: a survey. EURASIP Journal on Wireless Communications and Networking **2017**(1), 1–32 (2017). https://doi.org/10.1186/s13638-017-0806-6
38. Kang, H.J., Kang, C.G.: Mobile device-to-device (d2d) content delivery networking: A design and optimization framework. Journal of Communications and Networks **16**(5), 568–577 (2014). https://doi.org/10.1109/JCN.2014.000095
39. Lee, Y.L., Loo, J., Chuah, T.C., Wang, L.C.: Dynamic network slicing for multitenant heterogeneous cloud radio access networks. IEEE Transactions on Wireless Communications **17**(4), 2146–2161 (2018). https://doi.org/10.1109/TWC.2017.2789294
40. Leung-Yan-Cheong, S., Hellman, M.E.: The gaussian wire-tap channel. IEEE Transactions on Information Theory **24**(4), 451–456 (1978). https://doi.org/10.1109/TIT.1978.1055917
41. Liang, C.: Wireless virtualization for next generation mobile cellular networks. IEEE Wireless Communications Magazine **22**(1), 61–69 (2015). https://doi.org/10.1109/MWC.2015.7054720
42. Liang, C., Yu, F.R., Zhang, X.: Information-centric network function virtualization over 5g mobile wireless networks. Network, IEEE **29**(3), 68–74 (2015). https://doi.org/10.1109/MNET.2015.7113228
43. Liang, C., Yu, F.: Wireless network virtualization: A survey, some research issues and challenges. IEEE Communications Surveys & Tutorials **17**(1), 358–380 (2015). https://doi.org/10.1109/COMST.2014.2352118
44. Lichtman, M., Rao, R., Marojevic, V., Reed, J., Jover, R.P.: 5g nr jamming, spoofing, and sniffing: Threat assessment and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops). pp. 1–6. IEEE (2018)
45. Lin, X.: Cat: Building couples to early detect node compromise attack in wireless sensor networks. In: GLOBECOM 2009-2009 IEEE Global Telecommunications Conference. pp. 1–6. IEEE (2009). https://doi.org/10.1109/GLOCOM.2009.5425922
46. Lior, A., DeKok, A.: Remote authentication dial in user service (radius) protocol extensions. Rfc, IETF (2013), https://tools.ietf.org/html/rfc6929. (Accessed 05 February 2019)

47. Liu, D., Chen, B., Yang, C., Molisch, A.F.: Caching at the wireless edge: design aspects, challenges, and future directions. Communications Magazine, IEEE **54**(9), 22–28 (2016). https://doi.org/10.1109/MCOM.2016.7565183
48. Liu, H., Chen, Z., Tian, X., Wang, X., Tao, M.: On content-centric wireless delivery networks. IEEE Wireless Communications Magazine **21**(6), 118–125 (2014). https://doi.org/10.1109/MWC.2014.7000979
49. Loo, J., Aiash, M.: Challenges and solutions for secure information centric networks: A case study of the netinf architecture. Journal of Network and Computer Applications **50**, 64–72 (2015). https://doi.org/10.1016/j.jnca.2014.06.003
50. Mao, W.: Modern cryptography : theory and practice. Prentice Hall PTR, Upper Saddle River, N.J. (2004)
51. Martinez-Julia, P., Gomez-Skarmeta, A.: Using identities to achieve enhanced privacy in future content delivery networks. Computers and Electrical Engineering **38**(2), 346–355 (2012). https://doi.org/10.1016/j.compeleceng.2011.11.021
52. Nunes, I.O., Tsudik, G.: Krb-ccn: Lightweight authentication & access control for private content-centric networks. In: International Conference on Applied Cryptography and Network Security. pp. 598–15. Springer (2018)
53. Ohlman, B., Davies, E., Spirou, S., Pentikousis, K., Boggia, G.: Information-centric networking: Evaluation methodology. IETF (The Internet Engineering Task Force) Request for Comments (2014), https://tools.ietf.org/html/draft-irtf-icnrg-evaluation-methodology-01. (Accessed 05 January 2021)
54. Panaousis, E., Alpcan, T., Fereidooni, H., Conti, M.: Secure message delivery games for device-to-device communications. In: Poovendran, R., Saad, W. (eds.) Decision and Game Theory for Security. pp. 195–215. Springer International Publishing, Switzerland (2014). https://doi.org/10.1007/978-3-319-12601-2_11
55. Park, Y., Park, T.: A survey of security threats on 4g networks. In: IEEE Globecom Workshops. pp. 1–6. IEEE (2007). https://doi.org/10.1109/GLOCOMW.2007.4437813
56. Priya, V., Sakthisaravanan, B.: Information centric network for secure data transmission in dtn. In: International Confernce on Innovation Information in Computing Technologies. pp. 1–4. IEEE (2015). https://doi.org/10.1109/ICIICT.2015.7396101
57. Raheem, A., Lasebae, A., Aiash, M., Loo, J.: Supporting communications in the iots using the location/id split protocol: a security analysis. In: Second International Conference on Future Generation Communication Technologies (FGCT 2013). pp. 143–147. IEEE (2013)
58. Ravindran, R.: Enabling icn in 3gpp's 5g nextgen core architecture. IETF (The Internet Engineering Task Force) Request for Comments **2019**(Jan 5,) (2019), https://tools.ietf.org/id/draft-ravi-icnrg-5gc-icn-00.html. (Accessed 03 March 2021)
59. Ravindran, R., Chakraborti, A., Amin, S.O., Azgin, A., Wang, G.: 5g-icn: Delivering icn services over 5g using network slicing. IEEE Communications Magazine **55**(5), 101–107 (2017). https://doi.org/10.1109/MCOM.2017.1600938
60. Raykova, M., Lakhani, H., Kazmi, H., Gehani, A.: Decentralized authorization and privacy-enhanced routing for information-centric networks. In: Proceedings of the 31st Annual Computer Security Applications Conference. vol. 7-11-, pp. 31–40 (2015). https://doi.org/10.1145/2818000.2818001
61. RIFS, G.: Diameter roaming security - proposed permanent reference document. Tech. rep., GSMA (2016)

62. Shen, W., Hong, W., Cao, X., Yin, B., Shila, D.M., Cheng, Y.: Secure key establishment for device-to-device communications. In: IEEE Global Communications Conference (2014). https://doi.org/10.1109/GLOCOM.2014.7036830
63. Sun, J., Chen, X., Zhang, J., Zhang, Y., Zhang, J.: Synergy: A game-theoretical approach for cooperative key generation in wireless networks. In: IEEE INFOCOM 2014-IEEE Conference on Computer Communications. pp. 997–1005. IEEE (2014). https://doi.org/10.1109/INFOCOM.2014.6848029
64. Sun, L., Du, Q.: Physical layer security with its applications in 5g networks: A review. Communications, China **14**(12), 1–14 (2017). https://doi.org/10.1109/CC.2017.8246328
65. Tourani, R., Misra, S., Mick, T., Panwar, G.: Security, privacy, and access control in information-centric networking: A survey. IEEE Communications Surveys & Tutorials **20**(1), 566–600 (2018). https://doi.org/10.1109/COMST.2017.2749508
66. Tran, T.X., Hajisami, A., Pompili, D.: Cooperative hierarchical caching in 5g cloud radio access networks. IEEE Network **31**(4), 35–41 (2017). https://doi.org/10.1109/MNET.2017.1600307
67. Wang, K., Yu, F.R., Li, H., Li, Z.: Information-centric wireless networks with virtualization and d2d communications. IEEE Wireless Communications **24**(3), 104–111 (2017). https://doi.org/10.1109/MWC.2017.1500384WC
68. Wang, M., Yan, Z., Niemi, V.: Uaka-d2d: Universal authentication and key agreement protocol in d2d communications. Mobile Networks and Applications **22**(3), 510 (2017). https://doi.org/10.1007/s11036-017-0870-5
69. Wang, Y., Xu, M., Feng, Z., Li, Q., Li, Q.: Session-based access control in information-centric networks: Design and analyses. In: 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). pp. 1–8. IEEE (2014). https://doi.org/10.1109/PCCC.2014.7017094
70. Woo, T.Y., Lam, S.S.: Designing a distributed authorization service. In: Proceedings. IEEE INFOCOM'98, the Conference on Computer Communications. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Gateway to the 21st Century (Cat. No. 98. vol. 2, pp. 419–429. IEEE (1998)
71. Yi, X., Paulet, R., Bertino, E.: Private information retrieval. Synthesis Lectures on Information Security, Privacy, and Trust **4**(2), 1–114 (2013). https://doi.org/10.2200/S00524ED1V01Y201307SPT005
72. Yue, J., Ma, C., Yu, H., Zhou, W.: Secrecy-based access control for device-to-device communication underlaying cellular networks. Communications Letters, IEEE **17**(11), 2068–2071 (2013). https://doi.org/10.1109/LCOMM.2013.092813.131367
73. Zeltsan, Z.: Security architecture for systems providing end-to-end communications (2005), http://www.itu.int/ITU-T/worksem/ngn/200505/presentations/s5-zeltsan.pdf. (Accessed 05 January 2019)
74. Zhang, A., Chen, J., Hu, R.Q., Qian, Y.: Seds: Secure data sharing strategy for d2d communication in lte-advanced networks. IEEE Transactions on Vehicular Technology **65**(4), 2659–2672 (2016). https://doi.org/10.1109/TVT.2015.2416002
75. Zhang, T., Fan, H., Loo, J., Liu, D.: User preference aware caching deployment for device-to-device caching networks. IEEE Systems Journal **13**(1), 226–237 (2017)
76. Zhang, T., Fang, X., Liu, Y., Nallanathan, A.: Content-centric mobile edge caching. IEEE Access **8**, 11722–11731 (2019)
77. Zhang, X., Chang, K., Xiong, H., Wen, Y., Shi, G., Wang, G.: Towards name-based trust and security for content-centric network. In: 2011 19th IEEE International Conference on Network Protocols. pp. 1–6. IEEE (2011). https://doi.org/10.1109/ICNP.2011.6089053