Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2022.060110
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 31July 2022

Review report on Security Challenges in D2D communication

Ajith Kumar V[1]*, K Satyanarayan Reddy[2]

[1*] VTU RRC Belgaum, [2] ISE Department Cambridge Institute of Technology, Bangalore

ajith.it@gmail.com, ksatyanreddy@gmail.com

Abstract

D2D communication opens up a plethora of possibilities. In recent past there is a humongous growth in terms of mobile user subscription base. More and more applications are being ported over Internet, which can be accessed via mobile phones. D2D communication helps service provider by offloading traffic which otherwise use backbone network. D2D communication in 5G facilitates communication among heterogeneous devices, which might be constrained in terms of power and processing capabilities. This heterogenous connection presents challenge for securing D2D communication. Lightweight cryptography can be one of the options for security D2D communication. Lightweight cryptographic techniques help resource constrained devices to run cryptographic algorithms without compromising security requirements. In this way, secure D2D communication necessitates the use of lightweight cryptography.

Keywords: *Availability, Attack models, Communication Protocols, Confidentiality, Constrained devices, Denial of Service, Device to Device Communication, Integrity, Internet of Things, Lightweight Cryptography, User Equipment.*

1. Introduction

Device to Device (D2D) communication is a rapidly growing field with a wide range of applications. D2D communication combined with the Internet of Things (IOT) presents new security and privacy challenges. A lot of research is being done in this field, however, very nature of D2D communication, which is prone to information leakage. Rising use of smart phones and the Internet of Things (IOT), security breaches are becoming more regular. New attack vectors and a more dangerous threat landscape are emerging. Security and privacy are two important issues to consider. New revolution arose as a result of wireless mobile communication. Smart phones are impacting all aspects of society. Smart phones are now replacing computers. In a nutshell, we live in a connected world, which allows communication among disparate devices. Intelligent, smart, and connected devices are emerging. healthcare, disaster relief, and emergent situations, D2D communication is becoming increasingly common.

Even though the term D2D communication is very generic in usage, it covers various forms of communication such as V2V communication, M2M communication and communication among IoT enabled devices.

There are some similarities and differences between D2D communication and other forms such as Mobile Ad-hoc NETworks(MANET), and Cognitive Radio Networks (CRN). D2D communication might use infrastructure such as Cellular Networks in control plane, however this is absent in case of MANET and CRNs.

2. Evolution of D2D Communication

D2D communication in cellular networks is defined as direct communication between two mobile users without traversing the Base Station (BS) or core network. Device to Device communication is wireless and is different compared to Mobile Ad-hock Networks (MANETS). Figure 1 shows the classification of Device to Device communication. Basically, D2D communication can be broadly classified into two major categories. Inband D2D communication and Outband D2D communication. Inband D2D communication further classified into Underlay and Overlay. Underlay uses same radio resources for cellular communication and D2D communication. In this case there are some issues like interference and resource allocation. Various algorithms have been proposed for resolving interference issues, however in case of Overlay communication, it uses dedicated radio resources. Outband D2D communication does not use the same wireless channel for D2D, instead uses Wi-Fi Direct/Bluetooth/Zig-bee. Our focus is Outband D2D communication. It means devices should have 2 radio links one for Wireless and another for D2D communication using Wi-Fi Direct/Bluetooth/Zig-bee etc.

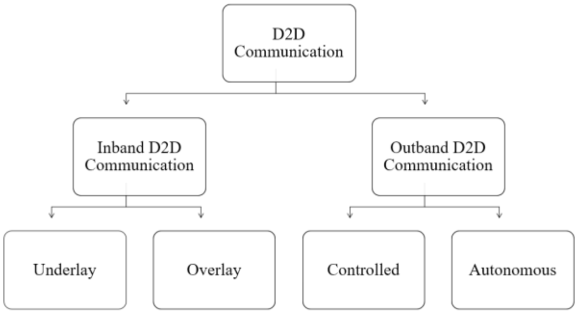

Figure 1: D2D Communication classification[1]

Outband D2D communication can be further classified into Controlled D2D communication, where Service Provider controlled the second link, in case of Outband Autonomous D2D communication second link which is used for D2D communication is controlled by end user not by the service provider. There are some challenges and advantages in D2D communication. Advantages are off-loading the communication from the centralized entity, saving the spectrum and bandwidth. Short range communications are typically characterized by higher throughput, lower delay and energy consumption when compared to long range communications[2].

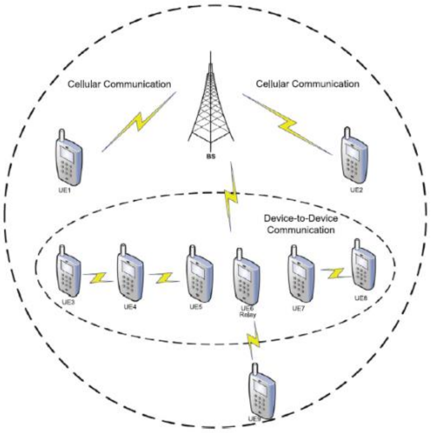

Figure 2: Cellular and D2D communication [3]

Figure 2 describes the difference between Cellular communication and Device to Device communication. In case of Cellular communication, two end users communicate with each other using the infrastructure provided by the service provider. However, in case of D2D communication, end users can use the infrastructure provided by service provider or they can communicate without using the infrastructure. Standardization bodies such as IEEE defined Wireless Standards related to data transmission speed and operating frequency. Table 1 provides details about Wireless Standards and related speed and operating frequency.

Table 1: 802.11 Wireless Standards

IEEE Standard	*Speed*	*Operating Frequency*
802.11a	Up to 54Mbps	5GHz
802.11b	Up to 11Mbps	2.4GHz
802.11g	Up to 54Mbps	2.4GHz
802.11n	Up to 600Mbps	2.4GHz

D2D communication can exist in various modes such as infrastructure less and infrastructure assisted. Some application such as file transfer between two mobile phones using Bluetooth as mode of communication does not require much infrastructure like routing device or intermediate gateway. However, it has other challenges such as device discovery, transmission power management.

Security for the data in transit is the major requirement in D2D communication. Since D2D communication inherits much of the characteristics of wireless communication, it is susceptible for various attacks such as Man-in-the-Middle(MITM), side channel attack, resource exhaustion attack which are common in any wireless communication. D2D communication need protection against all such attacks.

The term “Security” has threefold objectives to serve, defined in terms of Confidentiality, Integrity and Availability. Confidentiality can be ensured by encrypting the communication between sending and receiving devices, whereas Integrity ensures the message/data is not tampered during the transit, this can be achieved by computing hash of the message at the source and sending this along with the original message. At the receiving end once again, hash is recomputed on the received message. If both computed and received hash are same, then accept the message else discard the message. Availability refers to the availability of the system or resources for the valid users and tolerant against attacks from the intruders.

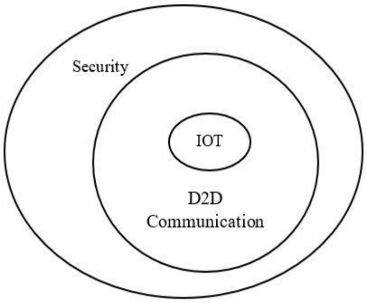

Figure 3: Securing view for D2D Communication

Security is a broad umbrella needed for the technologies like Internet Of Things (IOT), and D2D communication. We can also consider IOT as a special case of D2D communication.

Confidentiality can be assured by means of encryption. However, one can choose either public key cryptographic algorithm or private key cryptographic algorithm, Private key or symmetric key cryptography uses same key for encryption and decryption, whereas public key or asymmetric key algorithms uses key pair, public key for encryption and private key for decryption. Private key encryption is more efficient in terms of computation and memory requirements. However, secure key establishment between sender and receiver is a major issue. Public key encryption provides good security but computationally CPU and memory intensive.

Encryption algorithms used in wireless networks may not be well suited for the D2D environment. At the same time high volume of data exchange and sensitivity of the information poses security risks. Passive monitoring of wireless communication channel, unauthorized access to devices, device mismanagement which may result in unauthorized disclosure of sensitive information, these are some examples of possible attacks. These issues need to be taken into consideration while designing and selecting cryptographic algorithms for D2D communication.

3. Challenges in D2D Communication

There are many similarities between wireless communication and D2D communication. Due to the very nature of open-air interface, D2D communication prone to various attacks such as

3.1 Impersonate Attack

In this type of attack, a malicious attacker can pretend to be a legitimate user and intercept the communication between two legitimate users.

3.2 Denial of Service (DoS) attack

In case of DoS attack, the attacker can target victim by sending overwhelming connection requests, sometimes these requests cannot be handled by the victim's User Equipment(UE) and might result in reload or crash.

3.3 Password Guessing Attack

In this type of attack, the attacker can sniff the air interface and guess the encryption key by using brute force to break the encryption.

Above mentioned attacks can be mitigated by using Cryptography. Encryption for securing the data in transit. Authentication to defend against Impersonate attack and Checksum and Hashing techniques to defend against data modification attacks.

4. Overview of Lightweight Cryptography

Conventional cryptography may not be suitable for IoT. In this regard Lightweight Cryptography is very promising. National Institute of Standards and Technology (NIST) has decided to create a portfolio of lightweight algorithms through an open process. As per report NISTIR 8114 [9] , which provides an overview of lightweight cryptography, summarizes the findings of NIST's lightweight cryptography project, and outlines NIST's plans for the standardization of lightweight algorithms.

Lightweight cryptography targets variety of devices. Conventional cryptographic algorithms are best suited for PCs, tablets and smart phones. These set of devices does not require lightweight cryptography. On the other hand, lower spectrum devices such as Embedded Systems, RFID and Sensor networks may not be good candidate for conventional cryptography. Lightweight cryptography is primarily focused on the resource constrained devices that can be found at this end of the spectrum. In this category, we have wide variety of Microcontrollers which are available in 16-bit, and 32-bit.

Conventional Cryptography	**Servers and Desktops**
	Tablets and Smartphones
Lightweight Cryptography	**Embedded Systems**
	RFID
	Sensor Networks

Figure 4: Conventional and Lightweight Cryptography for various systems.

32-bit microcontrollers have a 32-bit address bus which provides access to up to 4 gigabytes (Gbytes) of memory. Traditional 16-bit microcontrollers have had 16 bits of addressing that can only access 64 kilobytes (Kbytes).

On some of these Micro-controller systems an extensive variety of instruction sets exists, which include a small variety of simple instructions. This small set of instructions may additionally result in many cycles to execute cryptographic algorithms.

Table 2: Crypgraphic Algorithms Profile Characteristics*

Physical characteristics	Area (in GEs, logic blocks, or mm2) Memory (RAM/ROM) Implementation type (hardware, software, or both) Energy (J)
Performance characteristics	Latency(in clock cycles or time) Throughput (cycles per byte) Power (W)
Security characteristics	Minimum security strength (bits) Attack models (e.g., related key, multi-key)

*Report on Lightweight Cryptography National Institute of Standards and Technology Internal Report 8114

For a few micro-controllers the quantity of This could result in slow processing or large amount of energy consumption while providing security for intended applications. In IoT type of environment wherein real-time processing of data is required. Random Access Memory (RAM) and Read Only Memory (ROM) can be a limiting factor. NIST's approach to evaluating and recommending algorithms is based on profiles that consist of a set of design goals, physical properties of the target devices, application-imposed performance characteristics, and security requirements. Cryptographic algorithms can be designed for specific purposes. NIST profiles based on device classes and target applications, not only considering specific applications. Profiles will be useful for a variety of applications.

Profiling is an important task based on a series of questions that need to be answered. This checklist is intended to serve as a starting point for understanding applications, identifying key bottlenecks, if any, and helping to identify additional limitations that may not be apparent at this point of time.

The development of the profile is based on the target application and the type of functionality that the application requires, such as encryption, authentication, hash and signature. If application is already using a cryptographic algorithm, need to consider why new algorithm is needed. In some places an estimate is required to replace the existing one with a new cryptographic algorithm. In some cases, a particular application may contemplate hardware implementation, or a software implementation, or combination of hardware and software implementation of the cryptographic algorithm.

5. Standards for Lightweight Cryptography

According to the ISO / IEC 29192 [9] standard, lightweight cryptography is a six-part standard that specifies lightweight cryptographic algorithms for confidentiality, authentication, identification, non-repudiation, and key exchange. Part 1 contains general information such as security, classification, and implementation requirements. Part 2 specifies the PRESENT and CLEFIA block ciphers. In 2014, an addition to Part 2 was proposed to include the SIMON and SPECK block ciphers with different key and block size combinations. As we know, PRESENT is specifically designed for low cost devices like RFID tags. CLEFIA is a highly efficient block cipher, especially on hardware. The SIMON and SPECK block cipher families were specially developed to provide security on constrained devices.

As specified in standardization document [9], first working drafts of the amendments with SIMON and SPECK were started in 2015, Part 3 of the standard specified the stream ciphers Enocoro and Trivium, whereas part 4 specified asymmetric techniques which includes identification scheme cryptoGPS, authentication and key exchange scheme ALIKE, and ID-based signature scheme. An addition to Part 4 included an Elliptic Curve based authentication scheme called ELLI. Part 5 specifies three hash functions: PHOTON, SPONGENT, and LesamntaLW. Part 6 is dedicated to MACs.

Additional standards are being developed to help resource constrained devices[9], to name few, Automatic identification and data capture techniques, which provides security services for RFID air interface communication. Part 1 describes the architecture, security features, and security service requirements for RFID devices. Cipher suites are defined in additional parts. Eight suites are currently being released specifying the use of AES-128, PRESENT-80, ECCDH, Grain-128A, AES OFB, ECDSA-ECDH, crypto-GPS and RAMON security services for air interface communication.

CRYPTREC [6] is the Japanese government's cryptography research and evaluation committee established to evaluate and recommend cryptographic techniques for government and industrial use. It is comparable in many respects to the European Union's NESSIE project and the US National Institute of Standards and Technology's Advanced Encryption Standard process.

CRYPTREC publishes three types of cipher lists: E-Government Recommended Ciphers List, List of Recommended Ciphers for Candidates and List of Monitored Ciphers. CRYPTREC's Lightweight Cryptography working group, founded in 2013, aims to research and support light weight cryptography solutions suitable for e-government systems and all applications where lightweight solutions are required. The task force examines state-of-the-art research in lightweight cryptography and its applications, conducts implementation evaluations, and as a result published a report in 2015.

6. Lightweight Ciphers

In this section we are going to discuss various lightweight cryptographic ciphers, HASH functions, and Message Authentication Codes (MACs).

6.1 Lightweight Block Ciphers

Various lightweight block ciphers have been proposed to provide performance advantages over NIST's Advanced Encryption Standard (AES), in particular AES-128. Some of these ciphers were developed by simplifying traditional and well-analyzed block ciphers to improve their efficiency. For example, DESL is a variant of DES in which the round function uses a single S-box instead of eight and skips the beginning and ending permutations to improve the size of the hardware implementation. Alternatively, some of the algorithms are dedicated block ciphers that have been designed from the ground up. PRESENT is one of the first lightweight block encryption designs proposed for limited hardware environments. SIMON and SPECK are families of lightweight block ciphers that are designed for simple, flexible, and powerful hardware and software. There are also algorithms from the 1990s like RC5, TEA, and XTEA that are made up of simple round structures that make them suitable for constrained software environments.

The performance advantages of lightweight block ciphers over traditional block ciphers are achieved through lightweight design options such as smaller block sizes smaller key sizes and simpler rounds.

6.1.1 Smaller Block Sizes

In order to save memory, light block ciphers can use smaller block sizes than AES (for example, 64-bit or 80-bit instead of 128-bit). As we are aware, use of small blocks reduces the limits on the maximum number of plaintext blocks to be encrypted. For example, the outputs of a 64-bit block cipher can be distinguished from a random sequence by using approximately 232 blocks for some of the allowed modes of operation. Depending on the algorithm, this can lead to attacks such as clear text recovery or key recovery or with non-negligible probabilities.

6.1.2 Smaller Key Sizes

Some lightweight block ciphers use small key sizes such as less than 96 bits, for example, PRESENT uses 80-bits key size for efficiency reasons, which is comparable with the minimum key size required by NIST of 112 bits.

6.1.3 Simpler Rounds

The components and operations used in lightweight block ciphers are generally simpler than those of conventional block ciphers. In lightweight designs with S-boxes, 4 bit S-boxes are preferred over 8 bit S-boxes. This reduction in size leads to considerable space savings. For example, the 4 bit S-box used in PRESENT required 28 Gate Equivalent (GEs), while the S-box AES required 395 GEs.

6.2 NIST Approved Block Ciphers

There are two NIST approved block encryption algorithms, AES and the Triple Data Encryption Algorithm (TDEA). The AES block cipher family comprises the three variants AES-128, AES-192, and AES-256, which support key sizes of 128, 192, or 256 bits.

All AES variants have a 128-bit block size. For lightweight cryptography purposes, AES-128 is the most suitable variant of the family due to the number of rounds and the size of the key plan. Existing compact implementations of AES-128 require 2090 GEs from to 2400 GEs. AES is designed primarily for software applications. Using 8-bit AVR micro controllers, encryption was achieved in 124.6 cycles per byte and decryption in 181.3 cycles per byte with a code size of less than 2 Kbytes. AES works very well on certain 8-bit microcontrollers, making it a good choice for these platforms. However, it is not possible to implement AES (or TDEA) encryption and decryption functions simultaneously on a 16-bit Renesas RL78 microcontroller if the ROM size is limited to 512 bytes and the RAM is limited to 128 bytes. For applications where the performance of AES is acceptable, AES should be used.

6.3 Lightweight Message Authentication Codes

A message authentication code (MAC) generates a label from a message and a secret key, which is used to verify the authenticity and integrity of the message. Label sizes of at least 64 bits are recommended for typical applications. For certain applications, such as Voice over IP (VoIP), the occasional acceptance of an inauthentic message may have limited impact on the security of the application, so after careful consideration, shorter labels may be used. Chaskey TuLP and LightMAC are some of the examples of lightweight MAC algorithms.

6.4 Lightweight Stream Ciphers

Stream ciphers are also promising primitives for restricted environments. The eSTREAM contest organized by the European Network of Excellence in Cryptology aimed to identify new stream ciphers that might be suitable for wide acceptance. Competition finalists were announced in 2008 and included three stream ciphers for resource-limited hardware applications. Grain is fully tested and offers deployment flexibility and also has a version that supports authentication.

6.5 Hash Functions

NIST-approved hash functions are specified in two Federal Information Processing Standard (FIPS) documents: FIPS 1804 specifies SHA13 and the SHA2 family (namely, SHA224, SHA256, SHA384, SHA512, SHA512 / 224, and SHA512 / 256) and FIPS 202 specifies the SHA3-based family permutation (namely SHA3224, SHA3256, SHA3384, and SHA3512). Neither of these approved hash functions is suitable for use in highly restricted environments, mainly due to their high internal state size requirements. Ideguchi et al. [8], examined the RAM requirements of SHA256, SHA512, and various SHA3 candidates on low-cost 8-bit microcontrollers and found that none of the NIST-approved hashing functions could be implemented within 64 bytes of RAM. The SHA3 family internal state variable is primarily determined by the width of the underlying 1600-bit permutation. FIPS 202 also defines smaller permutations with 25, 50, 100, 200, 400, and 800 bits; Some of these variants can be used later to define lightweight variants of SHA3, but these smaller variants are not currently approved for use in hash functions. A third block cipher, Skipjack, is only approved for legacy use decryption. SHA1 is not approved for all common applications of a hash function.

6.6 Authenticated Encryption Algorithms and MACs

Authenticated encryption algorithms offer advantages in terms of performance and resource requirements because they simultaneously provide confidentiality and integrity protection of messages. NIST endorses the CCM and GCM block encryption modes, which allow authentication and encryption simultaneously. NIST also approves separate MACs, CMACs, GMACs, and HMACs that are used to generate and verify tags to provide message authentication.

7. Conclusion

D2D Communication is going to be popular and widely adopted by the community. D2D communication facilitates direct communication between two User Equipment (UEs) without using much depending on the service provider. In a way D2D communication will offload some of the traffic from the service provider core network. This makes D2D communication as a preferred choice. Security is a major requirement for D2D communication as it inherits most of the characteristics of wireless communication, hence, similar security consideration is required. D2D communication is susceptible for various attacks. D2D communication security requirements also depend on User Equipment (UEs) characteristics, most of the UEs are limited by power and computational capabilities. In such cases Lightweight cryptography can be a good candidate. Lightweight cryptography has received increasing attentions from both academic and industry in the past two decades. A large number of lightweight algorithms have been proposed such as PRESENT, CLEFIA, LED, KANTAN, etc. In this work, an attempt is made to review most popular lightweight cryptography solutions over resource constrained devices. Analysis is done comparing the strengths and limitations, which encompasses the Security challenges in D2D communication. This analysis helps in choosing the right security for the D2D communication.

References

1. A. Asadi, Q. Wang, V. Mancuso, A Survey on Device-to-Device Communication in Cellular Networks, IEEE Communications Surveys & Tutorials, Vol.16, 2014, pp. 1801-1819. https://doi.org/10.1109/COMST.2014.2319555

2. A. Zhang, J. Chen, R. Q. Hu, Y. Qian, SeDS: Secure Data Sharing Strategy for D2D Communication, IEEE Transactions on Vehicular Technology, Vol.65, No.4, 2016, pp. 2659-2672. https://doi.org/10.1109/TVT.2015.2416002

3. A. Zhang, L. Wang, X. Ye, X. Lin, Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems, IEEE Transactions on Information Forensics and Security, Vol.12, No.3, 2017, pp.662-675. https://doi.org/10.1109/TIFS.2016.2631950

4. Akhil Kaushik, Satvika, Manoj Barnela, Anant Kumar, Keyless User Defined Optimal Security Encryption, International Journal of Computer and Electrical Engineering, Vol.4, 2012, pp.99-103.

5. C. Chen, K. Wang, T. Wu, J. Pan, H. Sun, A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices, IEEE Transactions on Information Forensics and Security, Vol.8, No.8, 2013, pp. 1318-1330. https://doi.org/10.1109/TIFS.2013.2270106

6. CRYPTREC, Cryptography Research and Evaluation Committees, Oct 15, 2021. https://www.cryptrec.go.jp/en/method.html,

7. Höyhtyä M, Apilo O, Lasanen M, Review of Latest Advances in 3GPP Standardization: D2D Communication in 5G Systems and Its Energy Consumption Models, Future Internet, 2018, https://doi.org/10.3390/fi10010003

8. Ideguchi, Kota & Owada, Toru & Yoshida, Hirotaka. (2009), A Study on RAM Requirements of Various SHA-3 Candidates on Low-cost 8-bit CPUs, IACR Cryptology ePrint Archive. 2009.

9. ISO/IEC 29192-2: Information security-Lightweight cryptography - Part 2: Block ciphers, Oct 15, 2021 https://www.iso.org/standard/78477.html,

10. Javed, Yasir, Khan, Adnan, Major Security attacks in D2D Communication, Ubiquitous Computing and Communication Journal, Vol.1, 2019.

11. Meltem Sonmez Turan, Kerry A. McKay, Çağdaş Çalık, Donghoon Chang, Larry Bassham, Status Report on the First Round of the NIST Lightweight Cryptography Standard-ization Process NISTIR 8268, National Insti-tute of Standards and Technology, U.S. De-partment of Commerce, 2019, https://doi.org/10.6028/NIST.IR.8268

12. Wang. M, Yan. Z, A Survey on Security in D2D Communications, Mobile Networks and Applications, Vol.22, No.2, 2017, pp.195–208. https://doi.org/10.1007/s11036-016-0741-5

13. R. Sedidi, A. Kumar, Key exchange proto-cols for secure Device-to-Device (D2D) communication in 5G, Wireless Days (WD), 2016, pp.1-6. https://doi.org/10.1109/WD.2016.7461477

14. Sencun Zhu, S. Setia, S. Jajodia, Peng Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. IEEE Symposium on Security and Privacy, Proceedings, 2004, pp. 259-271. https://doi.org/10.1109/SECPRI.2004.1301328

15. Wei Xi, Xiang-Yang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, Kun Zhao, KEEP: Fast secret key extraction protocol for D2D communication, IEEE International Workshop on Quality of Service, IWQoS, 2014, pp.350-359. https://doi.org/10.1109/IWQoS.2014.6914340