ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Review and Comparative Analysis of Stream Cipher for LTE Technology

Gagandeep Kaur
M.Tech Scholar
University College of Engineering
Punjabi University, Patiala

Dr. Jaswinder Singh
Assistant Professor,
University College of Engineering,
Punjabi University, Patiala

Abstract: With the advancement in the telecommunication system, fast evolution in mobile communication has been observed. Besides this there are many applications in the wireless sensor network which needs limited resources such as low gate count, low power consumption, low memory etc. These applications are mobile phones, smart grids, electronic identity cards, and RFID (Radio Frequency Identification Devices) tags. In this paper, we have discussed about the evolution of communication technology from first generation to fourth generation. We have also studied the security issues of LTE (long Term Evolution) technology. We have surveyed the various stream ciphers and comparative analysis of the various stream ciphers has also been done. On the basis of comparative analysis we have provided the research direction for the future work.

***Keywords*:** LTE (Long Term Evolution), Stream ciphers, cryptanalysis

I. INTRODUCTION

From last few decades, we have observed the huge changes in communication technology. The evolution of wireless communication is known as "generations" started from 1980's known as first generation 1G mobile wireless communication system. This was based on analog technology known as AMPS (Advanced mobile phone system). 1G has channel capacity of 30 kHz and frequency band 824-894 MHz. It uses circuit switching. It was designed only for voice calls without data services. After 1G, in 1990's 2G was introduced as the first digital cellular system. This generation uses two modulation schemes CDMA and TDMA. 2G has speed of 64 kbps with bandwidth 30-200 KHz. 2G uses both the circuit and packet switching technique. It provides data transfer rate up to 144 kbps. In 2000, 3G was introduced as the next generation. 3G provides security feature such as Authentication that means network operator can authenticate the identity of subscriber making it infeasible to clone someone's mobile phone, Confidentiality means protects data, voice and sensitive information from the third party and Anonymity means protects against someone tracking user's location or identifying calls made to or from users by third party. Packet switching was the technique 3G uses to send data. For video chatting and for high speed internet it allows bandwidth 15-20 MHz at frequency range 21000 MHz. Evolution of GSM is also part of 3G. A new service global roaming is also launched in this generation. 3G provides security with three features mutual authentication means protecting against the wrong base station attack, Data integrity which means preserving the privacy between sender and receiver and Network to Network security.

LTE (Long Term Evolution) also referred to as 4G communication system is developed by 3rd Generation Partnership Project for secure and fast communication. LTE provides high communication feature such as bandwidth, data rates and switching techniques. Long Term Evolution technology is the packet-switched based network which provides high speed communication. The demand for new mobile services and advancement for radio interface to LTE have filled in as driver to develop the core network. A System Architecture Evolution was initiated at the same time when LTE development was started has driven in Evolved Packet Core (EPC). LTE Architecture provides secure communication than 2G and 3G mobile communication system by providing mutual authentication between User Equipment (UE) and MME (Mobile Management Entity).

In this paper, we have provided an overview of stream cipher and types of stream ciphers. Paper contains detailed explanation about the cryptanalysis of stream cipher. In the paper, we have briefly analyzed the various proposed stream ciphers and compared them on the basis of certain defined measures such as, Size of key, Cryptanalysis etc . We have also defined the limitations in concern with different ciphers. On the basis of comparative analysis of various stream ciphers, we have defined the research directions in stream cipher.

A. ISSUES IN LTE

There are various types of security issues in LTE technology discussed below:-

Location Leaks: In location leak, there are three different attacks that can constrain an LTE device into uncovering its location. In first two attacks, the passive or semi-passive attacker is able to localize the target user within about 2 km area. In the third attack, an active attacker can exploit the

vulnerabilities in the implementation of LTE Radio Resource Control (RRC) protocol to accurately uncover the area of the target user via GPS coordinates using base station signal strengths as observed by that User Equipment.

Denial of Service: In denial of service, there are three attacks where an active attacker can cause continuing firmly denial of services against of the target UE. In the primary attack, the target UE will be compelled for utilizing the 2G or 3G network rather than LTE network which can make it possible to mount 2G/3G-specifies attack against that UE. In second attack, the attacker can selectively bound a UE only to some types of services. The attacks are continuing firmly and quiet. An active denial of service attacks that can quietly and persistent downgrade the LTE devices preventing their access to LTE network or constrained them to the LTE services.

Distributed Denial-of-Service attack: In Distributed Denial-of-Service attack, the attacker uses two or three combined machines to generate the vast number of messages on the target machine. An attacker use a flood of controller bots managed through command and control centre distributed in different locations to start a large volume of such attack. DDoS attacks against the LTE core network can affect the entire mobility network's data services.[6]

Network Access Issue: To LTE network, UEs utilization EPS-AKA verification system to right the benefits done EPC center. Those principle point of the EPS-AKA verification will be with validate both those UE Furthermore organize to agrarian for keys. This methodology triggered Eventually Tom's perusing those networks, At the client tries on append to LTE system. When UE associates to MME by means of eNodeB, MME may be those key hubs which executes the starting verification motor and verifies the shared Confirmation the middle of hubs. It additionally validates the last checksum computed Eventually Tom's perusing the MME What's more UE. Unauthenticated right solicitations compel those organize with send the queries should MME starting with An compromised UE/eNodeB Furthermore thus should HSS considerably in front of those UE verification. It triggers hacker to propel pernicious denial-of –service strike under HSS administrations from an fake client utilizing radio jamming.

B. CRYPTOGRAPHIC ALGORITHM

The application such as LTE, RFID tags, microchips with restricted environment need the cryptographic algorithms which protects the information with minimum storage, operate at high speed and provides a high level security. Cryptography is the process to encrypt the plaintext to ciphertext using secret key so that the message should be read by only the intented receiver with privacy. Cryptographic algorithm solves the problems which are related to authentication, privacy and integrity. Cryptographic algorithms provide various aspects of security such as confidentiality and integrity for the information exchanged over network. Confidentiality means information should be secret that is provided by encryption algorithm. Integrity means information is sent by the intended receiver and no changes are made to the information when it is transferred over the channel. Cryptographic algorithms are of two types that is symmetric key cryptographic algorithm and asymmetric key cryptographic algorithm.

Symmetric key cryptographic algorithm is further categorized into two parts named as Stream cipher and block cipher. Block ciphers are the ciphers which permutes N-bit blocks of plaintext with the secret key and output the N-bit blocks of ciphertext. Stream cipher works serially by producing the pseudorandom bits known as the keystream bits. The keystream bits is XOR with the plaintext to produce the ciphertext. Stream cipher preferred over block cipher because it becomes ideal for devices with restricted environment in terms of space and power. The another reason to prefer a stream cipher is it does not suffer from error propagation as the block cipher does because in stream cipher each bit is independently encrypted/decrypted. Stream ciphers are fast, more secure and software efficient as compared to block cipher.

II. STREAM CIPHER

In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the keystream. It is used to secure the communication in applications where the plaintext length is either unknown or continuous, like network streams. They are typically fast, compact, and consume low power, making them an attractive choice for resource-constrained devices. Stream ciphers work on only a few bits at a time they have relatively low memory requirements. Whereas with stream ciphers bytes are individually encrypted with no connection to other chunks of data, they are not susceptible to noise in transmission, Stream ciphers are usually best for cases where the amount of data is either unknown, or continuous .The main part of stream cipher is keystream generator. The role of keystream generator is to take secret key K and public IV (initialization vector) as input and produce pseudorandom binary keystream sequence. There are total two phases first is initialization phase and second is keystream generation. In the initialization phase, key and IV as input produces the internal state component of keystream generator. In second phase, the internal state is updated using the state update function and after that the output function uses internal state to produce the output bit or word depending on stream cipher's design specification. The keystream produced by the keystream generator is used for encryption and decryption of the information. Encryption is done by XORing the plaintext with the keystream to produce

ciphertext. Decryption is done by XORing the ciphertext with keystream to recover plaintext.

Stream cipher is classified in two categories- ***Synchronous stream cipher*** *and* ***Self-Synchronous stream cipher****:*

Synchronous Stream cipher:-Synchronous stream ciphers update the internal state independently from the plaintext or ciphertext data. A sender and a receiver must be synchronized before encryption/ decryption takes place. In this, if a bit of the cipher text message is altered, only a single plaintext bit is affected. The advantage of using synchronous Stream cipher is that there is no error propagation during the transmission of the message for this type of symmetric encryption. That is if bit error occurs in the ciphertext during transmission it will effect only the corresponding bit in plaintext. The disadvantage of using synchronous stream cipher is if the synchronization between sender and receiver lost, the decryption process fails and can be regained only through additional techniques.

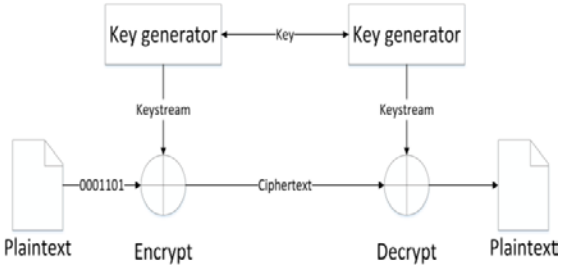

Fig 1. Synchronous stream cipher

Self-synchronous stream ciphers: Self-synchronizing stream ciphers update the internal state based on the N previous ciphertext bits. With self-synchronizing stream ciphers, the receiver can automatically synchronize herself with the sender after receiving N ciphertext digits. If a bit is altered, N plaintext bits will be affected. The advantage of self-synchronous stream cipher is if the synchronization lost due to ciphertext being inserted or deleted during transmission then it is capable of resynchronizing itself on receiving end. It is used where transmission of encrypted streams are long in length. The disadvantage of self-synchronization stream cipher is there is limited error propagation.

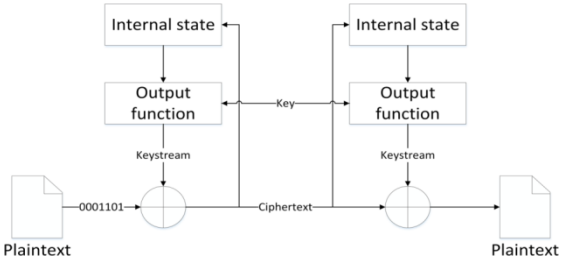

Fig 2. Asynchronous Stream Cipher

III. LITERATURE SURVEY

Hell, et al.[1] discussed Grain is the bit-oriented stream cipher whose design targets hardware environment where gate count, power consumption and memory is limited. Grain stream cipher uses two shift register, one with linear feedback and one with non-linear feedback and non-linear filter function. Grain uses 80-bit keys, 64-bit IVs and do not have explicit limit on number of keystream bits that should be generated for each key/IV pair and no attack faster than exhaustive key search has been identified. Grain bit-oriented stream cipher producing 1 bit/clock in its simplest implementation .If some additional hardware is used, it is very easy to increase the rate up to 16 bit/clock.[1]

Lin, et al.[2] proposed the GrainvI flow cipher is one of the seven finalists in the final eSTREAM portfolio. Though many attack(s) have been published, no retrieval attack better than exhaustive key search on full moon Caryopsis vI in the key setting has been found yet. In this report , new state recovery approach on Cereal vI utilizing the weak normality guild of the employed keystream production map in the cipher are proposed. These attacks have remarkable vantage in the offline time, online time and memory complexities, which are all better than exhaustive key search. The success probability of each new attack is 0.632. The proposed attack primarily depends on the order of weak normality of the employed keystream output function. This shows that the weak normality order should be carefully considered when designing the keystream output social function of Grain-like stream ciphers[2].

Johansson, et al.[3] proposed a new stream cipher , Grain-128, is proposed. The design is very small in hardware and it quarry environments with very limited resources .in gate count, power consumption, and chip area. Grain-128 supports key size of it of 128 bits and Quatern size of 96 bits. The design is very simple and based on two shift registry , one linear and one non linear, and an output signal role[3]**.**

Argen, et al.[4] proposed a comprehensive view of new stream cipher called Grain128a with optional authentication. Grain128a is the new member in the grain family which uses 128-bit key and 96-bit IVs. Grain128a is more expensive but offers more security as compared to other members of grain family. It has new feature of authentication mechanism same as used in ZUC cipher 128-bit EIA3 of 3GPP family. Grain128-a uses same building one linear feedback shift register, one non-linear feedback shift register and pre-output function[4].

Ghizlane Orhanou and Said El-Hajji [5] proposed a new set of cryptographic algorithms is being proposed for inclusion in the ”4G” mobile standard called LTE (Long Term Evolution), and the algorithms are open for public evaluation. The new set of confidentiality and integrity

algorithms EEA3/EIA3 is based on the new stream cipher ZUC. In this paper, verification and the implementation as well as performing the analytical analysis of the two algorithms, as they have done, with the first two sets of the LTE cryptographic algorithms EEA1/EIA1 and EEA2/EIA2. The verification of the confidentiality algorithm results on a correction of the proposed 3GPP algorithm code to meet the specifications requirements.[5]**.**

Altaf, et al.[6] discussed, Mobile communication system are now an essential of life throughout the world. Fourth generation "Long Term Evolution" (LTE) mobile communicating networks are being deployed. The LTE suite of specification is considered to be significantly better than its precursor not only in terms of functionality but also with obedience to security and privacy for subscribers. We carefully analyzed LTE access net protocol specifications and uncovered several vulnerabilities. Using commercial LTE mobile devices in real LTE networks, we demonstrate inexpensive, and practical attacks exploiting these vulnerabilities. Our first division of attacks consists of three different ways of making an LTE device leak its location: In our experiment, a semifinal -passive attacker can locate an LTE device within a 2km area in a urban center whereas an active attacker can precisely locate an LTE device using Synonyms/Hypernyms (Ordered by Estimated Frequency) of noun gp co-ordinates or trilateration via cell-column signal military capability entropy . Our second class of attacks can persistently deny some or all services to a quarry LTE device. To the best of our noesis , our work constitutes the first publicly reported practical attacks against LTE access network protocol[6].

Alyaa Ghanim Sulaiman and Imad Fakhri Al Shaikhli[7] provided the brief information about the cryptographic algorithms which contains three sets, each set contains pair of encryption algorithm and integrity algorithm which is based on core algorithm. Then these three set of cryptographic algorithm with their core algorithm are compared based on some factors. On basis of this comparison, this paper provided us the advantages and disadvantages of these algorithms.[7]

Frederik Armknecht and Vasily Mikhalev[8] proposed a new stream cipher with shorter internal state called Sprout which exploit the fact that storing same secret key consumes small area. The author decided to involve the secret key not only in initialization process but also in keystream generation phase. Sprout is based on Grain 128a. Sprout uses key size and IV of 80-bits. In sprout this keystream generator composed of two feedback shift register of 40-bits one LFSR and NFSR, an initialization function and an update function both key-dependent and of an output function that produces keystream. The basic idea behind Sprout is where the set of internal state is split into a large number of equivalence classes such that any tradeoff attack can consider every class atleast once.[8]

Virginie Lallemand and Mar´ıa Naya-Plasencia[9] proposed a new method for reducing the internal state size of stream cipher registers has been proposed in FSE 2015, allowing to reduce the area in hardware implementations. Along with it, an instantiated proposal of a cipher was also proposed: Sprout. In this paper, we analyze the security of Sprout, and we propose an attack that recovers the whole key more than 210 times faster than exhaustive search and has very low data complexity. The attack can be seen as a divide-and-conquer evolved technique that exploits the non-linear influence of the key bits on the update function. We have implemented the attack on a toy version of Sprout, that conserves the main properties exploited in the attack. The attack completely matches the expected complexities predicted by our theoretical cryptanalysis, which proves its validity. We believe that our attack shows that a more careful analysis should be done in order to instantiate the proposed design method[9]

Ghafari, et al.[10] discussed, After sprout stream cipher, new ultra-lightweight stream cipher called fruit is introduced. Fruit is extended from Grain v1 and Sprout by making the internal states more shorter with resistance from classical time-memory-data tradeoff attack .The main aim of this new stream cipher is to show how it is possible to exploit a secret key in design part as well because design is the part of internal state to achieve smaller area size. This idea is proved to be helpful for designers to extend the internal state upto key bits. In other words this stream cipher stores the key for reuse by different IVs or storing a key at fixed memory in some applications. Those applications are RFIDS or sim cards in mobile phones.[10]

Hamann et al[11] presents the most recent stream cipher which is known as Lizard is introduced for power constrained devices that is passive RFID tags. Lizard introduced with new features of 120-bit keys, 64-bit IVs and has an inner state length of 121 bit which is supposed to provide 80-bit security against key recovery attacks. Lizard allows to generate up to 2^18 keystream bits per key/IV pair, which would be sufficient for many existing communication scenarios like Bluetooth, WLAN or HTTPs. It is hardware efficient because it results by merging a Grain-like design with the FP(1)-mode, a recently suggested construction principle for the state initialization of stream ciphers, which offers provable 2/3n-provable security against TMD tradeoff attacks aiming at key recovery. This paper proves that lizard consumes 16 percent less power than Grain v1 with less area requirement. This indicates that in scenarios where plaintext packets of moderate length are to be encrypted under individual IVs, the FP(1)-mode provides an interesting alternative to conventional state initialization algorithms of stream cipher.[11]

Table1: Comparison Table

NAME OF STREAM CIPHER	YEAR/AUTHOR	SIZE OF KEY AND IV	TECHNIQUE OVERVIEW	CRYPTANALYSIS	LIMITATION
Grainv0	2004 Martin Hell, Thomas johansson, Willi Miere	Grainv0 contains key size 80-bits and IV of 64-bits.	Grain uses two registers-Linear Feedback shift register(LFSR) of 80-bit and Non Linear Feedback shift register(NLFSR) of 80-bit and Non Linear filter function	Correlation attack Algebraic attack Time/memory/data tradeoff attack Chosen IV attack Fault Attack	In Grainv0 the filter function was quite small only 5 variables and 12-non linearity.
Grainv1	2006 Martin Hell, Thomas Johansson, Willi Miere	In Grainv1 key size is 80-bit and IV is 64-bits.	In Grainv1 one bit of the 80-bit NLFSR and four bits of the 80-bit LFSR are supplied to a nonlinear 5-to-1 Boolean function and the output is linearly combined with 7 bits of the 80-bit NLFSR and released as output.	Correlation attack Algebraic attack Time/memory/data tradeoff attack Chosen IV attack Fault Attack	In Grainv1 weak key-IV pair which lead to self-sliding attack. Key initialization should be modified. Not feasible with exhaustive key search.
Grain128	2006 Martin Hell, Thomas Johansson, Willi Miere	Grain128 uses 128-bit key and 96-bit IV.	In Grain128, 128-bit key is loaded into NFSR and 90-bit IV is loaded into LFSR. Then cipher is clocked 256 times such that output function is fed back and XORed with input to LFSR and NFSR	Linear approximation attack Time/Memory/Data/ tradeoff attack Fault attack Algebraic attack	Hardware complexity. Insecure stream cipher
Grain 128a	2011 Martin Hell, Thomas Johansson, Willi Miere	Grain128 a uses key size of 128-bit and IV of 96-bits with optional authentication	Grain 128-a has pre-output stream which contains three functions namely LFSR , NLFSR and pre-output function. It has two modes of operation with or without authentication	Side-channel Attack Weak key-IV pair Fault Attack Algebraic Attack TMDTO Attack	Grain 128-a is expensive than grain128. Grain128-a needs more hardware to increase the speed.
Snow 3G	2012 Thomas Johansson and Patrik Ekdhal	Snow 3G uses 128-bit key and 128-bit IV.	SNOW 3G contains LFSR and a Finite State Machine (FSM). Snow3G is two component	Fault attack Weak-key IV pair Algebraic attack. Guess and determine attack	Snow3G is less secure stream cipher. Quite expensive. Slow in speed.

			stream cipher with an internal state 608 bits initialized by a 128-bit key and 128-bit IV.		
ZUC	2013 Zu chongzhi	In ZUC, the length of key and IV is same that is 128-bits.	ZUC cipher has three components:- LFSR, bit-reorganization and non-linear function f. ZUC has 128-bit key and 128-bit IV. It has two stages- initialization stage and working stage.	Timing Attack:- Side channel attack Cache timing attack	Attacks found may be certificational. Improve the attack to search key bits by examining the cases where end carry is generated twice.
Sprout	2015 Frederik Armknecht, Vasily Mikhalev	Sprout contains key size of 80-bits and IV size also 80-bits.	In Sprout, internal state is divided into two equivalence classes such that TMTDO attack consider it atleast once.	Time/memory/data/ tradeoff attack Guess and Determine attack Chosen IV Attacks Dynamic cube attack Weak key-IV Pair	Sprout was unsuccessful against the key-recovery attack. This key-recovery attack exploits the small size of registers and non-linear influence of key in the update function.
Fruit	2016 Vahid Amin Ghafari, honggang Hu, Ying chen	In Fruit key size and IV size is 80-bits.	Fruit stream cipher contain 43-bit LFSR and 37-bit NFSR in the internal state. It uses register of shorter length	Time/Memroy/Data Tradeoff Attack Linear Approx. Attack Related-key attack Cube attack Algebraic attack Fault attack	Ultra-lightweight stream cipher. Fruit provides the more resistance against the time/memory /data tradeoff attack. Fruit is considered to be secure stream cipher
Lizard	2017 Matthias Hamann, Willi Meier	In Lizard the size of key is 120 bits and size of IV is 64-bits.	Lizard stream cipher has internal state of 121-bit which contain two registers LFSR and NFSR. Both are of same length.	Exhaustive key search Time/memory/data tradeoff attack Correlation attack Algebraic attack.	The problem in Lizard is the the long guaranteed keystream period.

IV. RESEARCH DIRECTION

From the detailed survey of various stream ciphers it is found that the overall security of stream cipher depends on the following things:

1. The security of stream cipher depends on the randomness of key and IV. So at each round key and IV should update automatically and should be as unique as possible.

2. The second point on which security depends is Execution time for the stream cipher should be less. Delays are not acceptable.

V. CONCLUSION

Long Term Evolution is considered as the latest technology in mobile communication system which offers more capacity and speed as compared to other generations of mobile network. LTE is packet based scenario where packets are of variable size. This paper discussed about the attacks on the availability of LTE such as location leaks, denial-of-service, Distributed denial-of-service attacks. In order to resolve those attacks we have studied about the cryptographic algorithm which uses two types of ciphers

which are named as block ciphers and stream ciphers. As we know LTE uses packet switched scenario so we prefer the stream cipher algorithms. This paper has surveyed the comparative analysis of various stream ciphers and concluded that overall security depends on randomness of key/IV and execution time.

References

[1] M. Hell, T. Johansson, and W. Meier, “Grain - A Stream Cipher for Constrained Environments.”

[2] L. Ding, C. Jin, J. Guant, S. Zhangt, J. Lp, H. Wang, and W. Zhao, “Cipher New State Recovery Attacks on the Grain v1 Stream” no. November, 2016.

[3] M. Hell, T. Johansson, A. Maximov, and W. Meier, “A Stream Cipher Proposal Grain -128” pp. 1614–1618, 2006.

[4] M. Hell, T. Johansson, and W. Meier, “A New Version of Grain-128 with Authentication.”

[5] A. Mathematics and A. Evaluation, “The New LTE Cryptographic Algorithms EEA3 and EIA3” vol. 2390, no. 6, pp. 2385–2390, 2013.

[6] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. Seifert, “Practical Attacks Against Privacy and Availability in 4G / LTE Mobile Communication Systems," pp. 21-24, February 2016.

[7] A. G. Sulaiman, I. Fakhri, and A. Shaikhli, “Comparative Study on 4G/LTE Cryptographic Algorithms Based on Different Factors” vol. 5, no. 7, pp. 5–8, 2014.

[8] F. Armknecht and V. Mikhalev, “On Lightweight Stream Ciphers with Shorter Internal States.”

[9] V. Lallemand, “Cryptanalysis of Full Sprout”

[10] V. A. Ghafari, H. Hu, and Y. Chen, “FruitUltra - Lightweight Stream Cipher with Shorter Internal State” 2015.

[11] M. Hamann, M. Krause, and W. Meier, “LIZARD – A Lightweight Stream Cipher for Power-constrained Devices” pp. 1–34, 2012.