IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Cluster Based Secured Data Transmission using Hybrid Cryptography Techniques in Wireless Sensor Network

V.Perumal[1*], K. Meenakshi Sundaram [2]

[1]Dept. of Computer Science, Erode Arts and Science College, Erode-638 009, Tamilnadu, India.
[2]Dept. of Computer Science Erode Arts and Science College, Erode-638 009, Tamilnadu, India.

[*]*Corresponding Author: rishiperumal89@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i5.12711276 | Available online at: www.ijcseonline.org

Accepted: 19/May/2019, Published: 31/May/2019

Abstract— Security in the Wireless Sensor Network plays an important role and can be achieved by cryptographic algorithms. The cryptography is the science and art of transforming messages to make them secure and immune to attacks by authenticating the sender and receiver within the network. The Proposed methodology, hybrid cryptographic technique has combined Blowfish algorithm for symmetric and Elliptic Curve Diffie-Hellman algorithm for asymmetric. Blowfish algorithm provides high speed encryption process when compared with the other symmetric algorithms. The Elliptic Curve Diffie-Hellman algorithm combines the concept of elliptic curve and Diffie-Hellman key exchange algorithm. Hence, it provides more security compared to other asymmetric algorithm and the key exchange mechanism. Cluster based trust Management approaches are used to identify unauthorized user in WSN. It first identifies the trusted nodes in networks, then send packets through that trusted nodes. Trusted nodes are identified based on trust values to identify the neighboring nodes during verification process for improving the Packet Delivery Ratio and Energy Consumption.

Keywords— Sensor node, Elliptic Curve, Blowfish, Diffie-Hellman, Trust Node Calculation, WSN.

I. INTRODUCTION

WSN, each sensor nodes are collects the information from its nearby environment within its range. The collected information is further processed in its processing model, and then sent to the Base station. Every sensor node duplicates its energy while transmitting, receiving and processing. Forming sensor clusters is an effective way to improve scalability and longevity of wireless sensor network (WSN). However, security is a challenging issue in cluster-based WSNs, since sensors are usually deployed in unattended environments. Moreover, limited memory, processing power and communication range of sensor nodes (SNs) make traditional cryptographic schemes infeasible. Cluster heads (CHs) are usually responsible for data aggregation and consume more energy than the member nodes, which cause early termination from energy exhaustion. Furthermore, data decryption and encryption to ensure secure transmission demand more computation and hence shorten the network life.

1.1 Security Requirements- The Aim of security services in WSN is to protect the information resources from attacks and misbehavior. The security requirement in WSN include

Authentication: Receiver can determine the origin of the message and intruder cannot cover-up.

Integrity: Receiver should be able to verify that the message has not been modified in transit and intruder cannot substitute a false message for the original.

Non-Repudiation: A sender should not be able to falsely deny that he sent a message.

Confidentiality: A message may be encrypted so that others cannot read its contents.

Availability: It ensures that services and information are accessed when required. In sensor networks, there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks.

1.2 Cryptography- Cryptography enables to store sensitive information or transmits it across insecure networks. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptology embraces both cryptography and cryptanalysis. A cryptographic algorithm or cipher is a mathematical function used in the encryption and decryption process and cryptographic algorithm works in combination with a key – a word, number, or phrase – to encrypt the plaintext. The same plaintext encrypts different cipher text with different keys. The security of encrypted data is entirely dependent on two things. i.e the strength of the cryptographic algorithm and the secrecy of the key. Cryptography can be classified into two categories namely conventional cryptography and public-key

cryptography. In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.

1.3 Cryptographic Technique- The most appropriate cryptographic technique is important because cryptography ensures all the security requirements. To meet the constraints of sensor nodes, cryptographic techniques used in WSNs should be evaluated by code size, data size, processing time and power consumption. The computational capacity and memory capabilities of sensor nodes are limited, so the traditional cryptographic technique cannot be simply transferred to WSNs. In WSN to classify them into symmetric and Asymmetric cryptographic secret is required [KRI16]. There are number of secret sharing schemes techniques, namely symmetric and Asymmetric cryptographic.

Conventional Cryptography- The symmetric key algorithms are AES, DES, Trible-DES, Blowfish and Two fish, etc.

Public-Key Cryptography- Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption and a public key which encrypts data and a corresponding private or secret key for decryption.

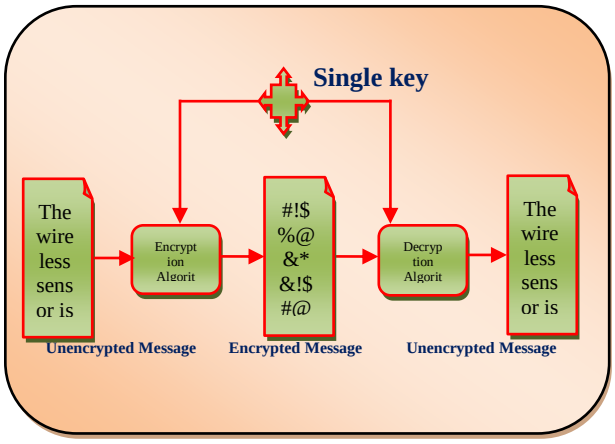

Figure 1.1: Symmetric Encryption and Decryption

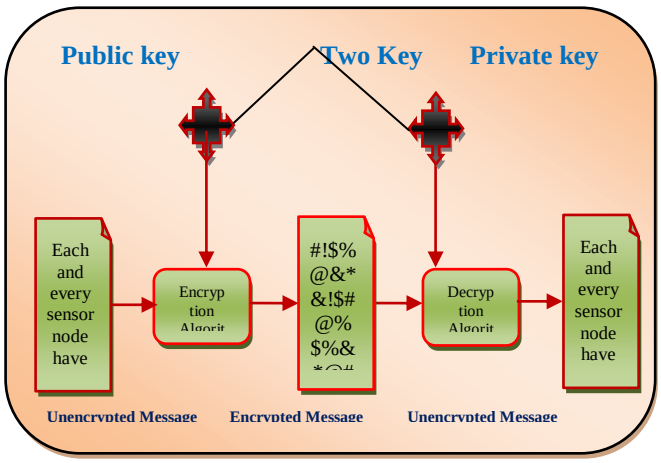

Figure 1.2 Asymmetric Key Encryption and Decryption

The asymmetric key algorithms are DSA, RSA, Elliptic curve, Diffie-Hellman etc.,

II. LITERATURE SURVEY

Asha Rani Mishra et al., [ASH12] identified that improved ECC is an appropriate choice to achieve security in Wireless sensor networks (WSN). ECC is an excellent choice for asymmetric cryptography in portable constrained devices. 1024-bit RSA key provides the same level of security as a 160-bit elliptic curve key. The advantages can be achieved from smaller key sizes including storage, speed and efficient use of power and bandwidth.

Madhumita Panda [MAD14] developed wireless sensor network that suffers from many constraints such as limited energy, processing capability, and storage capacity etc. There are many ways to provide security and one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches.

Kamulu Deepthi et al., [KAM16] proposed that for security to the data in WSN, various techniques have been studied in this survey. The survey provides that security to the data is the two-way key management between base station and cluster heads and from cluster heads to the sensor nodes by using ECC along with the concept of secret sharing scheme which not only avoids the single user authority but improves the security to the data.

Mohamed Elhoseny et al., [MOH16] explained that ECC is used to generate public and private keys for sensor nodes. The encryption key at each sensor node is 176-bits and is produced by combining the ECC key, identification number, and distance to its CH. To prevent the CH energy consumption as well as CH compromised attack, homomorphic encryption is used to allow CH to aggregate the encrypted data of its cluster members without having to decrypt them, to produce the final message that will be sent to the base station.

Abdullah Smadi et al., [ABD17] suggested in an estimate of the communication energy consumption for homogeneous wireless sensor security using DH-EKE public key agreement scheme in terms of variable key sizes and neighbour nodes. Hence, the proposed work helps the low power cryptographic system designers to be exposed for larger alterable schemes with variable techniques. The energy analysis results showed that the communication energy consumption of WSN is largely affected by the encryption/decryption key sizes and the number of neighbouring node as well as the sensor node features.

Preetika Joshi et al., [PRE15] proposed node to node authentication protocol with the concept of cryptography and cluster head that resolves the weakness of Diffie-Hellman key exchange scheme. This work completely eliminates the man-in-middle attack and the salient advantage of this work is addressing the challenging security issues of runtime phase

by real time key, which can efficiently protect the network against attacks of eavesdropping or captured nodes compromise and so on. Also, this scheme gives better performance in terms of connectivity, computation and storage or memory usage when compared with the EG-schemes and integrates WSN security with a promising protocol that provides more security and more efficiency.

Chaitali Haldankar et al.,[CHA14] suggested cryptographic algorithms like AES and Blowfish and compared different parameters and then did further implementation since the implementation of encryption/decryption algorithm is the most essential part of the secure communication. The algorithms are further considered for VLSI implementation. The evaluation is performed in terms of encryption speed, the CPU utilization with time and the battery power consumption. Results show the superiority of Blowfish algorithm with AES in terms of throughput and processing time. More the throughput, more the speed of the algorithm and less will be the power consumption.

Shamina Ross et al., [SHA17] developed Blowfish algorithm by enhancing its performance in terms of Speed, Throughput, Power consumption and Avalanche effect and proposed a way to enhance the performance of the Blowfish cryptography algorithm by introducing parallel processing technique and making modifications to the Fiestel (F) function of Blowfish by combining the Blowfish and the Runge-kutta (RK) Method. The F function of Blowfish has been modified with different formulae and the outcome of a series of RK-Blowfish algorithms were compared with the Blowfish algorithm. The enhanced performances of RK-Blowfish series of algorithms are reported. This work is useful in most consumer electronic appliances involved in data storage, transmission and communication ensuring data security.

III. Proposed Methodology

In WSN, the clusters represented that the information is shared in the cluster. So, unauthorized access is easily identified. For that, in this proposed work, Blowfish Elliptic curve Diffie Hellman (BECDH) hybrid cryptography algorithm is used and without using the secret key or wrongly accessed in the network then the acknowledgement is sent as malicious node. So, during this process the packets are required and information theft is presented.

This proposed hybrid cryptographic technique has combined Blowfish algorithm for symmetric and Elliptic Curve Diffie-Hellman algorithm for asymmetric. The Blowfish algorithm provides high speed encryption process when compared with the other symmetric algorithms. The Elliptic Curve Diffie-Hellman algorithm combines the concept of elliptic curve and Diffie-Hellman key exchange algorithm. Hence, it provides more security compared to other asymmetric algorithm and also the key exchange mechanism.

The proposed system hybrid cryptographic technique (BECDH) has high speed encryption and decryption process reduces the routing overhead and the key exchange mechanism eliminates the pre-distributed key requirement issues of the existing system in WSN.

3.1 Proposed Flow Diagram

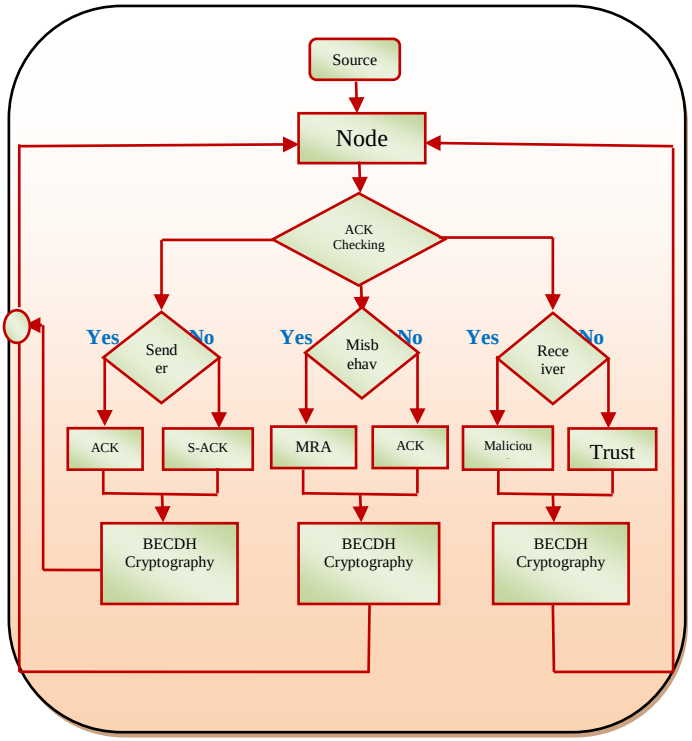

Figure 3.1 BECDH

The proposed system has three modes namely sender ACK, receiver ACK and misbehavior nodes ACK mode. Figure 3.1 shows the flow diagram of the proposed system-hybrid cryptographic technique (BECDH). All the three modes have sent acknowledgment packets to the network before encrypting the packets by hybrid cryptographic technique (BECDH). In receiver side, the encrypted information has been decrypted by the same hybrid cryptographic technique (BECDH), after which the receiver receives the original acknowledgment packets. In order to have security, all the acknowledgment packets are encrypted and decrypted using a private key and authentication can be obtained by asymmetric cryptography. Hence, the proposed hybrid cryptographic technique is a combination of asymmetric and symmetric cryptographic algorithm to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

3.2 Trust Node Calculation

In this secure data transmission based hybrid, cryptography technique is used in Intra cluster network. For the Intra cluster network, each sensor that is a member of the group calculates individual trust values for all group members. Based on the trust states of all group members, a CH detects the malicious nodes and forwards a report to the BS. The trust value is based on direct or indirect observation. Direct observations represent the number of successful and unsuccessful interactions. Indirect observations represent the recommendations of trusted peers about a specific node. Here, interaction means the cooperation of two nodes. For an example, a sender considers an interaction as successful if the sender receives an assurance that the packet is successfully received by the neighbor node and that node has forwarded the packet toward the destination in an unaltered fashion.

The wireless sensor network with 50 nodes is created in the NS-2.34 version. An energy model is used to calculate the energy of each node. Now the energy calculated for the nodes is compared with one another and the node with higher energy is found. This node with higher node energy is assumed as the cluster head. At the next step, the trust values of the 50 nodes are calculated considering the successful and unsuccessful transmissions. If the trust value of the node is 2 then the node is trusted node. If the trust value is other than 2, then the nodes are considered untrusted.

3.3 Experimentations and Results

The suggested hybrid Cryptography Technique is improved by Network simulator ($NS_{2.34}$) Environments. The proposed algorithm of BECDH is highlighting the network energy with new developed method RK-BLOFISH provides a good output with respect to the Trust node (or) which Intruder Finding, Encryption and Decryption process, Energy Savings, packet delivery ratio, End to End delay time and Throughput.

Simulation Parameters and Values

Parameters	Values
Number of Node	50
Area Dimension	400 * 400(Meter)
Routing Protocol	DSR
Total Energy	150 Joule
Threshold value	0.3 Joule
Maximum Packet Size	4000 bits
Total number of packet size	5000 bytes
Simulation Time	60 (seconds)
Type of the MAC	802.11
Simulation Tool	NS2.34

The proposed algorithm of BECDH is highlighting the network energy with new developed method RK-BLOFISH provides a good output with respect to the Trust node (or) which Intruder Finding, Encryption and Decryption process, Energy Savings, packet delivery ratio, End to End delay time and Throughput.

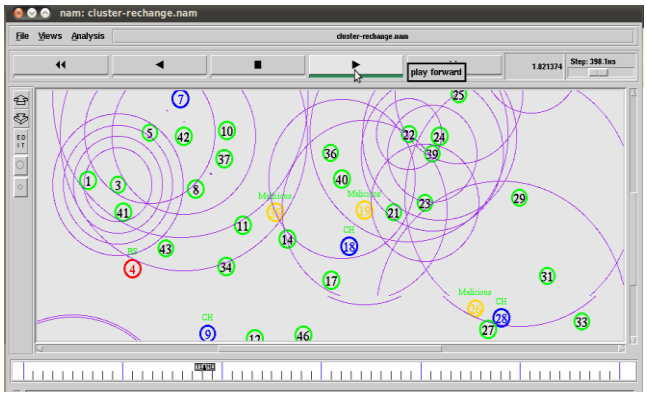

Fig.4

In Figure 4, green color nodes are the cluster members, red color node is base station, blue color nodes represent cluster head and yellow color nodes denote malicious node.

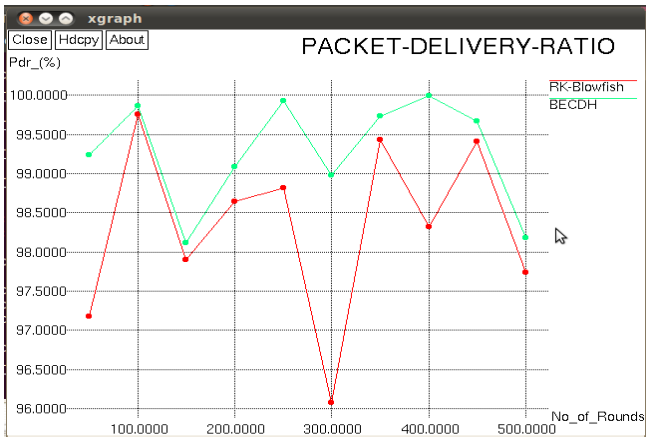

Figure.5

Figure 5 shows the result analysis of packet delivery ratio with respect to the time. The proposed BECDH technique provides better improvement in particular time for secured delivery of data than the existing RK-Blowfish technique. This is because the proposed BECDH techniques, Secret key and authentication are generated to securely deliver the packets with certain time. While transmitting the data in WSN, encryption and decryption are carried out with the help of key exchanging mechanism to reach the exact receiver node. Average of RK-Blowfish packet delivery ratio is 98.33% and proposed technique of BECDH is 99.28%. It is clear that BECDH provides good performances and minimizes the energy utilization.

Encryption

During encryption, the time taken to convert Encrypted data to decrypt is defined as the encryption time.

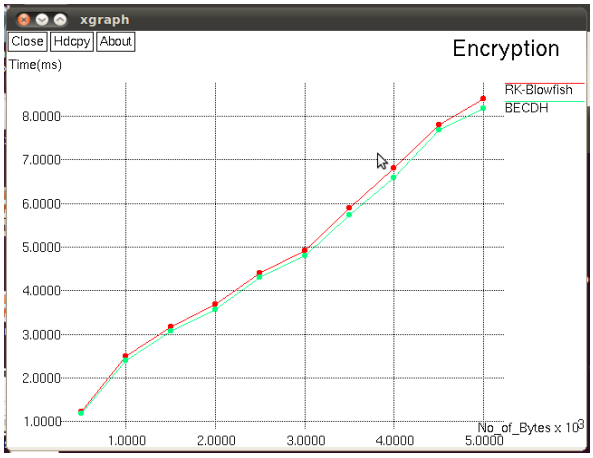

Figure.6

While comparing the result of existing method, RK-Blowfish denotes Encryption time is 8.398(ms) and the proposed method BECDH denotes 8.189(ms), these providing better than the existing method.

Decryption

During decryption, the time taken to convert Encrypted data to original data is defined as the decryption time.

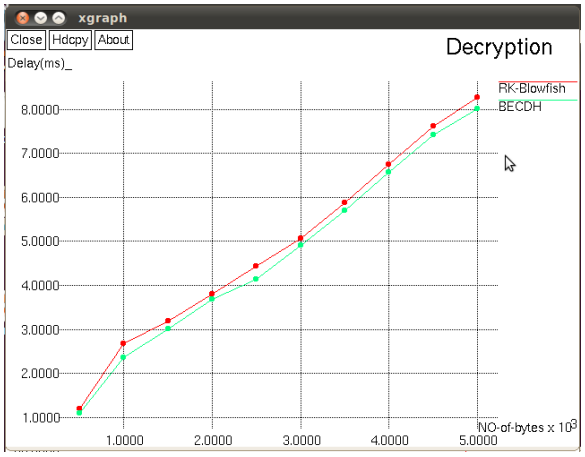

Figure.7

From the comparison of the result of existing method, RK-Blowfish decryption time is 8.268(ms) and the proposed method BECDH has 8.013 (ms). This difference makes the proposed method better.

V.CONCLUSION

Security is the most important issues in wireless network. Using this proposed approach, trust management protocol is used to identify the trusted nodes with malicious node. Then secured and efficient way of data transmission are directed and communicated to any kind of networks re confirmed here.

The BECDH algorithm reduces the execution time and provides better security and it consumes less memory usage compared to any other algorithm. Compared to traditional cryptosystems like RSA, Blowfish, ECDH and etc., BECDH offers smaller key sizes, lower power consumption, as well as bandwidth savings. The third party is not possible to obtain the shared secret key of BECDH algorithm. So the BECDH algorithm appears to offer equal security for a smaller key size and therefore reduces processing time of the Wireless Sensor network.

VI. REFERENCES

[1]. Asha Rani Mishra, Mahesh Singh "Elliptic Curve Cryptography (ECC) For Security in Wireless sensor Network" *International Journal of Engineering Research and Technology* (IJERT), vol-1,Issue-3,may-2012.

[2]. Madhumita Panda "Security in Wireless Sensor Networks using Cryptographic Techniques" *American Journal of Engineering Research* (AJER) , Volume-03, Issue-01, pp(50-56)-2014.

[3]. kamulu Deepthi, Krishnachaitanya,.Katkam "Wireless Sensor Networks Security Survey Using Cryptography" *International Journal Of Emerging Trends & Technology In Computer Science* (IJETTCS), Volume 5, Issue 5, September - October 2016.

[4]. Mohamed Elhoseny , Hamdy Elminir , Alaa Riad , Xiaohui Yuan "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption" *Journal of King Saud University – Computer and Information Sciences*, pp(262–275), ELSEVIER-2016.

[5]. Abdullah Smadi, Hesham Enshasy, Qasem Abu Al-Haija "Estimating Energy Consumption of Diffie-Hellman Encrypted Key Exchange (DH-EKE) for Wireless Sensor Network" *International Conference On Intelligent Techniques In Control, Optimization And Signal Processing*, IEEE-2017.

[6]. Preetika Joshi, Manju verma, Pushpendra R Verma "Secure Authentication Approach Using DiffieHellman Key Exchange Algorithm for WSN" *International Conference on Control,Instrumentation, Communication and Computational Technologies* (lCCICCT), IEEE-2015.

[7].Chaitali Haldankar, Sonia Kuwelkar "IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM" *International Journal of Research in Engineering and Technology* (IJRET) , Volume-3 Special Issue-3,May- 2014 .

[8].Shamina Ross.B, Josephraj.V " Performance Enhancement of Blowfish Encryption Using RK-Blowfish Technique" *International Journal of Applied Engineering Research*(IJAER) , Volume 12, pp(9236-9244) – 2017.

[9].Rajat Soni, Deepak Sethi, Partha Pratim Bhattacharaya " ANALYSIS OF VARIOUS CRYPTOGRAPHIC ALGORITHMS FOR SECURITY IN WIRELESS SENSOR NETWORKS" *International Journal For Advance Research In Engineering And Technology*(IJARE), Volume-4, Issue-V, May-2016.

[10]. Juan Li "A Symmetric Cryptography Algorithm in Wireless Sensor Network Security" *International journal of online Engineering* ((iJOE) – Vol 13,2017.

[11]. Huang Lu, Jie Li, Mohsen Guizani "Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM* - 2013.

[12]. Thiruppathy Kesavan Venkatasam, Radhakrishnan Shanmugasundaram " Authentication in Wireless Sensor Networks

Using Dynamic Keying Technique" *International Journal of Intelligent Engineering and Systems* (IJIES), Vol.9, No.3, 2016.

[13]. Usha.A, Dr.Subramani.A "Performance Study of Key Developer Data Encryption and Decryption Algorithm (KDDEDA) with AES, DES and BLOWFISH" *International Journal Of Engineering And Computer Science* (IJEC), Volume 5, Issue 12, Pp(19596-19611), Dec- 2016.

