Use of Improved Rabin Algorithm for Designing Public Key Cryptosystem for Wireless Sensor Networks

Aaisha Jabeen Siddiqui, Praveen Sen, Aarti Ravindrasingh Thakur, Ashwini L. Gaur, Priyanka Chandrakant Waghmare

Abstract*— *Wireless Sensor Networks are one of the most popular areas of research now days. These types of networks have observed a wide variety of applications in security areas such as defense, ecological etc. These applications are highly dependent on monitoring sensitive information such as movement of particulars, detecting and tracking of location etc. Providing security in such complications has made Wireless Sensor Networks security a challenge. As sensor nodes are powered by batteries, energy efficiency becomes a critical aspect in such type of networks and because of this many security protocols proposed earlier for Wireless Sensor Networks are proved out to be expensive. In this paper, we have focused on a security protocol which provides a strong level security and also uses the battery of the sensor nodes efficiently. The proposed work is tested on confidentiality and integrity of data and authenticity in communication. This system tracks the location of sensor nodes and the location of the nodes will become the input for key generation phase. The communication between the server and the sensor will take place by encrypting the location address of the respected sensor.

Keywords*—*Security in WSN, Rabin public key cryptosystem, CRT, Java Eclipse, Android SDK.

I. INTRODUCTION

A wireless sensor network is a collection of wireless nodes that work in a cooperative manner. These nodes have self processing capabilities. They may contain different types of memory. They exchange information about their environments/ surroundings with each other or to a base station [1]. While doing this tremendous/ intense security is necessary if the application is used for military (sensing or) surveillance. The energy of the batteries has to be made to last as long as possible. The use of a cryptographically algorithm should save both time and energy.

Various other security algorithms implemented on WSNs have proved to be expensive and consume more energy.. WSNs are unprotected to various types of attacks or to node compromises that exploit various susceptibilities of protocols and threaten the authenticity, confidentiality and integrity of the information.

Encryption-Decryption algorithm is categorized as symmetric and asymmetric. Symmetric is a secret key algorithm which depends on single key. And Asymmetric algorithm is a public key cryptosystem which makes it harder at factorization.

Many asymmetric algorithms have been used for secure communication to wireless sensor networks. Because of the large keys used they take more execution time which uses up the batteries of the nodes. RSA and Ecliptic Curves, which are asymmetric algorithms implemented on WSNs, use large keys. Both require large prime numbers as input to the key generation phase and because of this take more execution time. An important aspect of WSNs is saving battery power. If we reduce the execution time of the algorithm, it will reduce battery power consumption.

The proposed algorithm Rabin is an asymmetric algorithm which is difficult at factorization/ to factorize. This system will first track the location of the sensor nodes, then their latitude and longitude value will become keys for encrypting the sensed data. For decryption, the Chinese remainder theorem is implemented, along with two modular exponentiations. As key size becomes small here, this system proves to be more efficient than any other security algorithm. Hence, for authenticity and non-repudiation security requirements, asymmetric algorithms are implemented on wireless sensor networks for hard mathematical factorization. [2], [3], [4], [5] are several public-key system protocols proposed for wireless sensor networks.

II. BACKGROUND AND RELATED WORK

We present a location based authentication protocol for sensors in a secure and efficient manner. Because it is location based key pairs will be different with any change in distance and direction. To give more prospective to our proposed authentication algorithm, this section review resulting performance of different protocols used for securing sensor nodes. A study in [2] shows that this paper has proposed a protocol based public key cryptography for outside entity authentication and session key generation.

Communication between the base station and the sensors is through private key cryptography and communication between external entity and base station is through public key cryptography.

Manuscript published on 28 February 2014.
***** Correspondence Author (s)

Ms Aaisha Jabeen Siddiqui, Computer Science & Engineering, Nagpur Institute of Technology Affliated to RTM Nagpur University, Nagpur, India.

Prof. Praveen Sen, Computer Science & Engineering, Nagpur Institute of Technology Affliated to RTM Nagpur University, Nagpur, India.

Ms Aarti Ravindrasingh Thakur, Computer Science & Engineering, Nagpur Institute of Technology Affliated to RTM Nagpur University, Nagpur, India.

Ms Ashwini L. Gour, Computer Science & Engineering, Nagpur Institute of Technology Affliated to RTM Nagpur University, Nagpur, India.

Ms Priyanka Chandrakant Waghmare, Computer Science & Engineering, Nagpur Institute of Technology Affliated to RTM Nagpur University, Nagpur, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

According to the paper, system can be prevented from node comprise attack and traffic analysis attack. In [3], symmetric key based protocol has been proposed for secure communication in wireless sensor networks.

This paper investigates various attacks on cluster base data gathering protocol and tries to give a symmetric key based solution to it. Analysis on paper results shows that attacks like spoofed, altered or replayed can be avoided by adopting a symmetric technique. This system is reliable only for smaller networks as single key usage can make guessing attacks strong.

In [4], Rabin public key cryptography is adopted for mobile network authentication. In this, mobile starts the protocol by sending its identification number to the server. The server stores mobile ID for the purpose of authentication. According to the algorithm, it selects large prime numbers as a key pair and transfers this to encryption phase. Cipher text is calculated by applying public key. Using CRT, validity of the cipher text is checked. Execution time taken by the algorithm is 20 ms/byte.

In [5], a study is conducted to investigate the fast developing security systems in the field of wireless information security. ECC's uses smaller key size to provide high security and high speed in a low bandwidth. Due to their difficulty in discrete logarithmic problem, execution time for ECC is 120 ms/byte according to the result comparison in [6].As wireless sensor nodes are battery dependant the system taking more time will not be efficient. The paper also discusses issues involved in implementing Elliptic Curve Cryptography (ECC). It provides a brief explanation about ECC basic theory, implementation, and also provides guidance for further reading by referring to cryptography techniques.

In paper [6], a 160 bit ECC processor is proposed. The implementation presented in this paper chooses an ECC based authentication technique with a key size of 160 bits as it provides strong security and can be used for a longer time. According to the paper, the time required by single point multiplication is good and the time consumed for single 160 bit multiplication at 10 MHz is 0.39 seconds.

In this paper [7], an Identity authentication scheme has been implemented in wireless peer-to-peer network. Proposed scheme apply a hybrid P2P topology and tickets issued by super peers to perform the user mutual authentication. Also presented a quick re-authentication technique dealing with non-permanent broken down link to simplify the authentication procedure and improve the efficiency. Scheme can resist most malicious attack effectively.

In [8], RSA public key cryptography has been proposed as a solution to security in wireless sensor networks. Although RSA uses large key size, execution time is more as compared to Rabin authentication algorithm proposed in []. According to comparative result RSA takes 40 ms/bytes to execute. RSA for wireless sensor networks proved out to be cost worthy and inefficient.

In this paper [9], Tiny PK authentication scheme have been proposed by Watloel. The security scheme is used to authenticate outside entity from network and allow the sensor nodes to share information with outside entity.

The scheme provides trusted certificate authority, which is a public key private key for the entity.

III. SECURITY REQUIREMENTS

The security system in WSNs should fall on the following requirements to satisfy the purity of the transmitted data. It should be protected while being transmitted to various public channels and resources [1], [2], [16].

A. *Data Confidentiality:*

This implies a relationship between the communicating nodes to keep the message confidential, so no other node should come between them. Various attacks such as traffic analysis attack can be restricted through keeping data confidential.

B. *Data Integrity:*

Protocol should ensure that no alteration or updating can be made on transmitted message. Message should appear at other end as it was transmitted.

C. *Data Authentication:*

Authenticity is the important aspect in WSNs. Protocol should ensure that data must be transmitted to the actual receiver. It also ensures that evidence received at the other end is correct and not tampered with.

D. *Data Freshness:*

Protocol should ensure that data transmitted is very recent and any attacker should not replay messages.

E. *Secure localization:*

Accurate location information is necessary to diagnose faults immediately. The Rabin location based algorithm gives accurate location information and also protects privacy of data.

IV. PROPOSED AUTHENTICATION PROTOCOL

The location based Rabin Public-Key cryptosystem is an asymmetric algorithm which uses different location parameters for each individual sensor node. Here, input will be different every time the sensor changes its position. Latitude and Longitude of sensors are calculated through GPS or other location tracking software or through manual configuration. The proposed Rabin algorithm is divided into four modules. First the sensors are located. After this, key pairs are generated using latitude and longitude of a wireless node. In the encryption module, cipher text is generated by applying public key. It is then transmitted to the receiver to check the validity.

With the help of Chinese Remainder Theorem, four squares modulo m1, m2, m3, m4 are calculated. If the value of the cipher text is equal to any of the square modulo then the login request is accepted, otherwise the login request is rejected. Chinese remainder theorem is a proven algorithm for strong authentication.

Hence, using the proposed algorithm will ensure confidentiality, integrity and authenticity of information transmitted within wireless sensor networks.

A. *Location Tracking Module*

Location based protocols have been adopted to take into account the position of each sensor node in a network. GPS can be used to track location in order to increase the level of data security.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

As each time distance and direction are changed, we always get different input keys.
Step I: Calculate Latitude and Longitude by using GPS or other location tracking software.
Step II: Take variable p=latitude and q=longitude.
Step III: Pass variable p & q to Key Generation Module.

B. *Key Generation Module:*

The system creates key pairs by following steps:
Step I: Compute n=p*q
Step II: System's public key is 'n' and system's private key is [p, q].
Step III: Send public key and private key to Encryption Module.

C. *Encryption Module:*

System creates cipher text by the following steps:
Step I: Receive key pairs.
Step II: Calculate Cipher text $C = M^2 \bmod n$.
Step III: Generate cipher text and send it to remote machine.

D. *Authentication Module:*

The system authenticates by checking the validity of the cipher text. Private keys are necessary to decode it. If both it and the location are known then the plain text belongs to the set of square roots generated through CRT. i.e $M\in\{0,\ldots,n-1\}$.
Following are the steps involved in the authentication phase:
Step I: Receive request C and checks for validity.
Step II: Apply Chinese remainder theorem for authenticity. Theorem states that for any set of integers and for given integers there exists commons modulo, which can be cipher text according to proposed scenario.
Step III:

$$X_1 = a_1 \pmod{m_1}$$
$$X_2 = a_2 \pmod{m_2}$$
$$\vdots$$
$$Xn = a_n \pmod{m_n}$$

has a unique solution mod $(m_1, m_2,\ldots,m_n)$
Where, $m_1, m_2,\ldots,m_n$ are the square modulus's generated by Chinese remainder theorem. If cipher text is equal to any of the square root value then accept the login request.
Step IV: Otherwise reject the login request.
Step V: The square roots are in the set [0,…, n-1]
Step VI: Among these square roots one is the original plaintext.

V. SYSTEM ARCHITECTURE

The idea behind above protocol is simple. Track location of sensor node using GPS or manual configuration. In step 1, latitude and longitude are calculated to generate key pairs. In step 2, Public key and private key are inserted in Encryption module to generate cipher text. In step 3, transfer cipher text to remote system, so that authenticity can be achieved.
In step 4, receiver after receiving cipher text, checks for its validity. Authentication is the key aspect of Rabin algorithm. Chinese remainder theorem will generate square moduli and check the value of C with these modulo. If match occur then accept login request otherwise reject login request. With the help of Chinese Remainder Theorem, four squares modulo m1, m2, m3, m4 are calculated. If the value of the cipher text is equal to any of the square modulo then the login request is accepted, otherwise the login request is rejected. Chinese remainder theorem is a proven algorithm for strong authentication. Hence, using the proposed algorithm will ensure confidentiality, integrity and authenticity of information transmitted within wireless sensor networks.
Here, standard Chinese remainder theorem is implemented for proving authenticity to the received message. Due to its location based nature, security attacks like secure localization can be easily overcome.

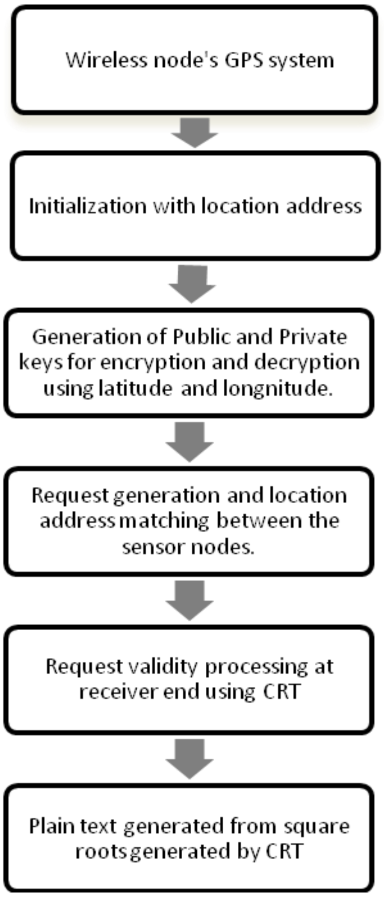

Wireless node's GPS system
Initialization with location address
Generation of Public and Private keys for encryption and decryption using latitude and longnitude.
Request generation and location address matching between the sensor nodes.
Request validity processing at receiver end using CRT
Plain text generated from square roots generated by CRT

Fig 1: Process Architecture

VI. ANALYSIS OF PROPOSED AUTHENTICATION PROTOCOL

In this section we introduce possible attacks take on Wireless sensor networks and steps taken on attack by proposed authentication algorithm.
A.*Monitoring and Eavesdropping*: This is the most common attack on privacy of data. By snooping the attacker can easily analyze the content of the transmitted data. Every transmission between sensor nodes and the base station is in encrypted form so no such attack is possible on WSNs with the proposed algorithm.
B.*Camouflage Adversaries*: In this, attackers can insert and hide their nodes into the sensor network. These nodes then copy normal nodes and transmit information on their behalf. This is prevented by the proposed algorithm as it is location based. Every node carries a different location address; therefore one cannot copy another node within the WSN.

VII. EVALUATION OF ALGORITHM

As Rabin cryptosystem is location based algorithm many attacks can be solved. The huge advantage of proposed algorithm is that multiple plaintexts can be recovered to generate cipher text. As data is represented in numeric value, it makes code breaking difficult.

The efficiency of algorithm can be calculated by encryption and decryption. For encryption location of particular node and square modulo of n is calculated, which make it hard at factorization, like security in RSA. For decryption, Chinese remainder theorem is applied, along with two modular exponentials.

VIII. IMPLEMENTATION AND RESULTS

We have used Android Development Tools (ADT) which is a plug-in for Eclipse IDE. ADT extends capabilities of Java Eclipse, which is excellent tool to run projects on Android environment. Idea behind using such setup is, Android tools create run time environment for project and one can easily demonstrate it on Android cell phones.

We have implemented location listener interface for calculating location of the sensor nodes. Experimental results show that text message is transferred between the nodes. Latitude and Longitude along with the text message take 1.2ms/byte time to execute. Total time required to execute encryption-decryption phase is 6ms.

Fig 2 shows performance analysis of execution time of Elliptic curve cryptographic algorithm, RSA and location based Rabin cryptosystem. According to the papers referred for ECC and RSA, both have provided security over communication on wireless sensor networks. They have taken parameter as long prime numbers along with the text message to transfer over communication channel in wireless sensor networks. Where, Rabin improved the parameter by accepting location of any sensor nodes.

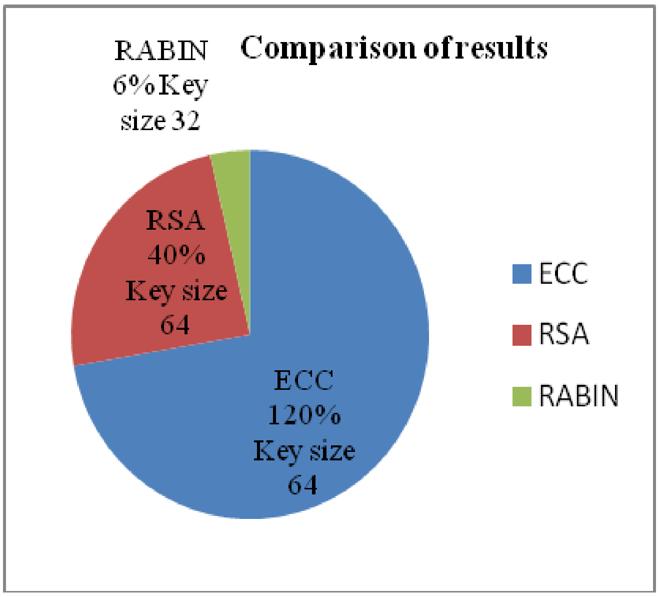
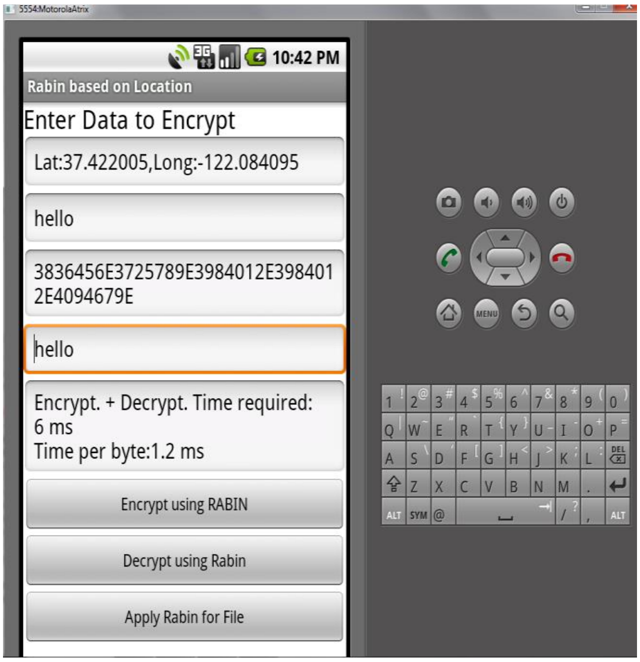


Fig 2: Performance of execution time of different algorithm.

Performance comparison is taken on key size of 64 for ECC ,64 for RSA and 32 key size for location based Rabin cryptosystem Fig 3 illustrates the instantaneous time taken to run location based Rabin cryptosystem algorithm with Android virtual device manager. Location is calculated through manual configuration as GPS systems are there in computer devices. After this, encryption and decryption phase is run in 6ms time.

We observe that due to time taken by this algorithm is very less compare to any other algorithm existed for WSNs security; it will take less battery power consumption.

We also have experimented Location based Rabin algorithm with large files. Performance analysis for the same is also less. It takes lesser time any other algorithm. Transmitting large files have disadvantage due to problem occur in wireless sensing nodes. As it requires battery power and more memory.



Enter Data to Encrypt

Lat:37.422005,Long:-122.084095

hello

3836456E3725789E3984012E398401
2E4094679E

hello

Encrypt. + Decrypt. Time required:
6 ms
Time per byte:1.2 ms

Fig 3 shows time taken to run Location based Rabin algorithm.

XI. CONCLUSION

Wireless sensor nodes have strict constraints on the resources, such as battery power and memory, and time efficiency. Minimizing the battery consumption, while maintaining a desirable level of security is very challenging task. In this paper we have proposed a location based security algorithm to calculate time efficiency and to authenticate received data. Our results shows that time taken by proposed authentication algorithm is very less as compare to any other algorithm exist for wireless sensor network security. Performance analysis shows that proposed authentication algorithm is secure and efficient. As this system is location dependant, it will be difficult for adversaries to track every time changing locations of a node. Hence, from experiments and results we can say that, proposed authentication algorithm is secure and efficient for wireless sensor networks security.

REFERENCES

[1] Garcia-Hernandez, C. F., Ibarguengoytia-Gonzalez, P. H and Perez-DiaZo J. A 'Wireless Sensor Networks and Applications: A Survey', IJCSNS, 7(3),264-273 (2007)

[2] V. C Shekhar, Mrudala Sarvabhatla , 'Security in WSNs with Public Key Techniques', ICCCI-(2012), Jan 10-12, Coimbatore, India

[3] P. Mohanty, N. Sarma, S. Panigrahi, S. S. Satapathy, 'A Symmetric Key based secured data gathering protocol for WSN', ICCCI-(2012), Jan 10-12, Coimbatore, India

[4] K .Saravana selvi T. "Rabin Public Key Cryptosystem for Mobile Authentication.". IEEE- (ICAESM -2012) March 30, 31, 2012.

[5] Dr. Lawrence Washington." Elliptic Curve Cryptography and Its Applications to Mobile Devices." Wendy Chou, University of Maryland, College Park. Department of Mathematics.

[6] Dr. R. Shanmugalakshmi ,"Research Issues on Elliptic Curve Cryptography and Its applications - IJCSNS, VOL.9 No.6, June 2009,

[7] Gaoxiang Chen, Gelian Song, Tao Zhuang, 'An identity Authentication Scheme in Wireless Peer-to-Peer Network', IEEE (2010), Oct 3, 2010

[8] Lein Harn & Thomas Kiesler "Two New Efficient Cryptosystems Based on Rabin's Scheme: Alternatives to RSA Cryptosystem ".Computer Science Telecommunications Program University of Missouri - Kansas City Kansas City, MO 64110. 1990 IEEE.

[9] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys '04), pp. 162-175, Baltimore, Md, USA, November 2004.

[10] S. Prasanna Ganesan " An Asymmetric Authentication Protocol for Mobile Devices Using HyperElliptic Curve Cryptography." India. 2010 IEEE.

[11] A Perrig, R Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.

[12] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable
communications system, " IEEE J. Set. Areas Commun. , vol. 11, pp. 821-829, 1993

[13] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and
Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89

[14] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems, " IEEE Trans. Wireless Communication. , vol. 4, no. 1, pp. 57-64, 2005.

[15] Jian-zhu Lu and Jipeng Zhou" On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks." Department of Computer Science University of Jinan Guangzhou, Guangdong, China 510632. 2010 IEEE

[16] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, 'A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks', (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

Ms Aaisha Jabeen Siddiqui, Student of Mtech Final Year studying in Nagpur Institute of Technology, Nagpur .She received the B.E degree in Computer Science and Engineering, from RTMNU, Nagpur in 2010. She has received progressive success in various Debate Competition and Elocution. Her main research interests include network securities, Cryptography, Database Management..

Prof. Praveen Sen, he is working as a Head of the Department in Information Technology, in Nagpur Institute of Technology . His various research paper has been published in various international Journal. He is member of various international journal committee. He has good grip in design, development and implementation of IT, Software tools. He has a good hand on various Programming languages. His main research interests include Android, Cryptography, Social Computing.

Ms Aarti Ravindrasingh Thakur, Student of Mtech Final Year studying in Nagpur Institute of Technology, Nagpur .She received the B.E degree in Computer Science and Engineering, from RTMNU, Nagpur in 2010. Her main research interests include network securities, Cryptography, Database Management..

Ms Ashwini L. Gour, she is a 2nd year Master of Technology fellow in Computer Science and Engineering , at Nagpur Institute of Technology, Maharashtra, India. .She received the B.E degree in Computer Technology, from RTMNU, Nagpur in 2011 and also P.G. diploma in Advanced Computing Course CDAC, from Sunbeam Institute of Technology, Karad Pune, India in August 2011. She has good grip in design, development and implementation of IT, Software tools. Her main research interests include network securities, social networks with applications to Social Computing.

Ms Priyanka Chandrakant Waghmare, Student of Mtech Final Year studying in Nagpur Institute of Technology, Nagpur. Attended three days National Workshop on "NETWORK SECURITY, OCT 2013" in B.D.C.O.E, Sewagram, Wardha. . Attended two days National Workshop on "OPEN SOURCING & its Utilization for Rural Development",at B.D.C.O.E, Sewagram, Wardha.