International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

CENTRALIZED SIGNATURE BASED APPROACH FOR WIRELESS SENSOR NETWORK USING RSA ALGORITHM

Megha Joshi[1], Saumil Patel[2]
[1]Post Graduate Student, [2]Assistant Professor, Department of Computer Science & Engineering,
Narnarayan Shastri Institute of Technology, Jetalpur, Ahmedabad - 382426

ABSTRACT: Now a day, Wireless Sensor Networks (WSNs) are very popular. Even its popularity increasing rapidly as development in processor and sensor power increases. Newly developed sensors are highly flexible according to application and uses new energy reducing method. However security is still remained burning and unresolved issues for centralized and decentralized wireless sensor environment. Using various theoretical and practical analyses, various security challenges and security attacks have been traced out. And so efficient protocol designed called SET-CRA have been designed to provide efficient security against various security attacks and challenges in non-clustered wireless sensor network environments. Previously proposed scheme, TESLA and µ-TESLA has limited in scopes; those schemes provide only provide protection against basic security attacks like non-repudiation. But scheme SET-CRA scheme provides flexibility against numerous security attacks. This scheme ensures protection against different range of security attacks and provides secure and efficient transmission in centralized wireless sensor environment.

GENERAL TERMS: Security, Authenticity
KEYWORDS: Centralized, secure and efficient data transmission protocol, FND (First Node Dies) time, LND (Last Node Dies) time, RSA Cryptography.

I. INTRODUCTION

Wireless sensor networks are gathering of several of autonomous sensor nodes with intend of wireless communication. It comprises of sensor equipped nodes called motes or simply sensors which reports collected data from one or more trusted gateway nodes by sensing the environment physically [3]. Such individual nodes are spatially distributed to sense and monitor the physical changes of the surrounding environment and they are also capable to communicate in wireless sensor network in two ways: centralized and decentralized. Centralized means such data processing and transfer can be carried out through or via the medium of base station in WSNs. Whereas in case of decentralized environments, sensor nodes are spatially distributed in different clusters and can only communicate with other sensor nodes with the help of cluster head presents in each of cluster head. Cluster of that cluster sends the received messages to a base station after receiving messages from neighbouring sensor nodes. However, it is feasible for sensor nodes to communicate with other surrounding nodes directly in non-clustered scenario but only after permission or required authentication done by base station(s). Generally in such non-clustered scenario, trust is major issue [2], so to commence trustworthy communication between the neighbouring sensor nodes it is important to do the pre-registration and authentication of all sensor nodes present in the network.

A. BACKGROUND AND MOTIVATION:

As different security applications have diverse security requirements, it is a challenging or almost invincible task to satisfy all the security requirements using single authentication protocol. Detailed literature depicts that numerous protocols have been proposed such as PEACH [13], RLEACH [17] which use similar concept of LEACH protocol [18]. Most of Leach like methodologies makes use of symmetric key management schemes for security but it is unable to provide defence against security attacks like cloning, selective forwarding, node capture, trust etc [1-8]. So to deal with different types of wireless environments, it is necessary to provide high level security to these kinds of networks with an efficient security framework or an upbeat protocol. So after performing rigorous theoretical and practical analysis of innumerable security challenges, attacks and detailed literature survey, an efficient protocol have been introduced called, 'SET-CRA' to provide secure and efficient transmission in centralized wireless sensor environments. In this research paper acronym 'high level security' has been used for the above mentioned security attacks. To increase level of protection, digital signature can be used as very effective mechanism in critical applications like military or government agencies. The concept of digital signature has been developed as a good authentication practice in WSNs for security. In proposed scheme, the protocol is divided in two stages: authentication and session Establishment. During the phase of authentication, sender sensor node will initiate the communication with the receiver sensor node by sending its own identity and other details encrypted with its private key. Moreover, receiver sensor node can always verify the details of sensor node with the base station anytime during the initiated communication link. Not only this, receiver sensor node can also verify sender sensor node's signature. In second phase, a unique session number will be generated and unique session key will be generated to establish a session between sender and receiver node. This protocol will protect sensor nodes to initiate or enter into the current session and protect the deployed wireless sensor network from variety of security attacks in terms of network lifetime. The remainder portion of this paper is organized as follow: section 2 describes the wireless

network arrangements, security preambles and vulnerabilities. Section 3 presents the details of the proposed SET-CRA protocol features and characteristics. Analysis and evaluation of the proposed protocol SET-CRA protocol has been discussed in Section 4. The last section concludes the proposed protocol.

II. NETWORK PROTOCOL ARRANGEMENTS AND PREEMBLES

A. WIRELESS SENSOR NETWORK ARRANGEMENTS

Here, it is considered a wireless sensor network which consists of variety wireless sensor motes and a base station(s). It is assumed that the base station is always reliable and a trusted authority. Also, all surrounding sensor nodes may be compromised by the variety of security attacks and such high-level security attacks also affect the data transmission between sensor nodes and a base station. In case of centralized environment, base station is the central entity and it is responsible for data aggregation and storage. In this environment, sensor nodes can communicate with surrounding sensor nodes via the medium of base station(s). Whereas in clustered WSNs, sensor nodes are divided into homogeneous cluster and communication can be done via cluster-head (CH) of as individual cluster via the medium of base station. In all these cases, thus it is prudent to switch the sensor nodes into sleep or inactive mode when it is not sending or receiving any data for saving energy. In this paper proposed protocol SET-CRA has been designed for centralized-non clustered wireless sensor network.

B. PROTOCOL PREEMBLE AND VULNERABILITY

According to previous research work, it is analysed that protocol used in WSNs are vulnerable to a variety of security attacks like cloning, node capture etc. Such attacks may results in serious damage to the network and may lead to huge packet loss. If an attacker manages to compromise or pretend to be an original sensor node, it can hassle such high level attack and results in disrupting the network. In addition, an attacker may intend to inject malicious packets in the deployed WSN and can transmit confidential information outside the network. To provide defence against all these attacks it is designed an efficient protocol called SET-CRA, which is robust against insider an outsider attacks than other type of protocol in WSNs. The characteristics of the proposed scheme mitigate the attacking risks and increase the headache of an attacker to identify and compromise important nodes present in WSNs. The primary objective of the proposed protocol SET CTA is to guarantee a secure and efficient data transmission between neighbouring sensor nodes and base stations(s). Most of the previous research works on secure transmission protocols for wireless sensor networks are not capable to provide strong protection against newly evolved security attacks. In this paper, it is endeavour to solve this problem by using digital signature based crypto-system that guarantees and strong defence against variety of security attacks by also considering energy aware information exchange in WSNs.

III. PROPOSED SET-CRA SCHEME FOR WSNs

An IBS scheme implemented for WSNs consists of following operations: set up at base station, key extraction and signature signing of the data transmitting nodes, verification of the data receiving nodes. In this proposed protocol has used signature based algorithm which consists of four different processes such as initial system set up, key management, signature generation and signature verification.

A. PROPOSED PROTOCOL OPERATION

SET-CRA protocol operates in number of stages during communication. Each stage consists of an authentication phase and a session establishment phase.

System Initial set up

1. The step by step description of the proposed SET-CRA scheme is follows:
2. First of all, BS registers all valid sensor nodes and also generates private key for all registered nodes.
3. In addition, Base station also registers all the verified users and created their private keys.
4. When a sensor node A registers with the verified users and their private keys.
5. To provide the additional security against various attacks the BS sends registration information encrypted with the hash function H like (H (SIDX)).

Authentication Process

After successful registration of a sensor node, authentication process will be performed by the receiving nodes. In this scheme, authentication procedure, both sending and receiving sensor nodes will generate their session key. The session key generation procedure is as described in remainder part of this protocol. The steps for authentication process are shown in Fig. 1.

1. As shown in Fig. 1, sensor node X sends a communication request to sensor node Y. To initiate secure communication, communication message has been encrypted with the private key of the sending sensor node.
2. After receiving communication request, receiving node Y will verify the identity of the sending sensor node X.
3. After the authentication process, sensor node Y will reply by sending reply message which includes identity SIDY, signature S and message M encrypted with the encrypted with the secret key DIDY.
4. Sensor node X will perform the same step as step 2 and verify the registration of the sensor node X.

The proposed scheme has used certain terminologies. The meaning of terminologies is given in the following table 1.

Table 1: Different terminologies with their meaning used in SET-CRA protocol

MKBS	Master Secret Key For Base Station
SID_X	Identity of Sensor Node X
DID_X	Secret Key for Sensor Node X
PKBS	Public Key for Base Station
UIDi	Identity of User i
UPKi	Private Key of User i
M	Authentication Request Message
BS	Base Station
H	Hash function
SID_Y	Identity of Sensor Node for node Y
DID_Y	Secret Key for Sensor Node Y

SESSION KEY ESTABLISHMENT PROCESS

To increase the level of security, unique session key management scheme has been established for each session shown in Fig. 2

1. This process will be initiated by selecting random number and compute the Temporary Session Key TSK encrypted with the hash function.
2. After receiving session establishment request, sensor node Y will generate a shared secret key KYX and compare it with KXY to check it is matching or not.
3. If it is matching, sensor node Y will compute the session establishment key Sk = KDF (KXY) using the key generation function KDF which is based on RSA algorithm [7][11].

RSA_Key_generation_Function {select two large prime numbers a and b such that a ≠ b,
η□ □a*b
Φ (η) = (a-1) (b-1)
Select e such that 1<e< (η) and e is co prime to Φ (η)
c □ □e-1 mod Φ (η) □// c is inverse modulo Φ (η)
Public Key□ (e, n) //to be announced publicly
Private Key □c // to be kept secret Return public key and private key}

1. Match $K_{XY} = K_{YX}$? if both are same, then compute S_k.
2. Now, we can use the established session key to secure a session between sensor node X and Y. It will also provide additional security to manage concurrency so third party sensor node or intruder cannot enter the session and perform attacks like node capture, cloning etc.

IV. SET-CRA SCHEME FOR WSNs

A. Protocol Characteristics

After performing strict theoretical and practical analysis of SET-CRA protocol and analysed characteristics of proposed protocol are summarized shown below.

4.1.1 Communication Overhead

Proposed Protocol delivers and provides assurance of less communication overheads as it is executed in centralized environment and important aspects and mechanisms are stored on the central entity.

4.1.2 Computation Overhead

The protocol is designed in such way that also provides assurance about different computations and efficient transmission between two sensor motes and key distribution centre.

4.1.3 Protection against Security attacks and Authentication

SET-CRA is much focused and delivers higher level security against malicious attacks and secure authentication procedure to achieve security goal and strong authentication is followed.

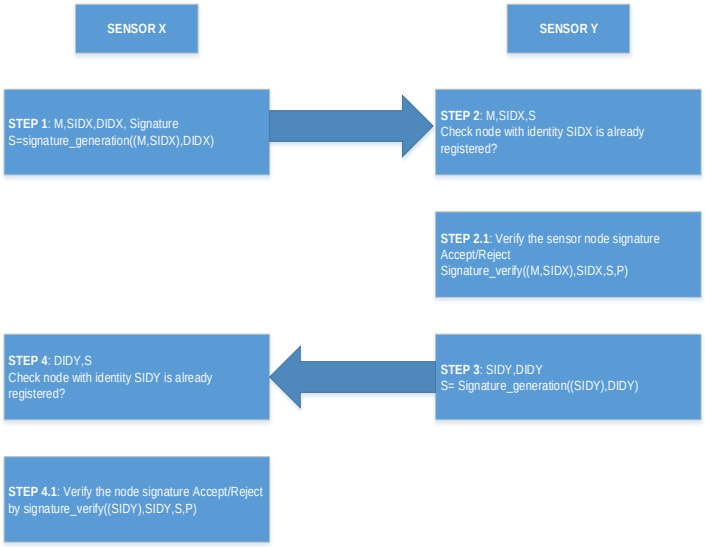

Fig. 1: Authentication process of sensor node X with sensor node Y

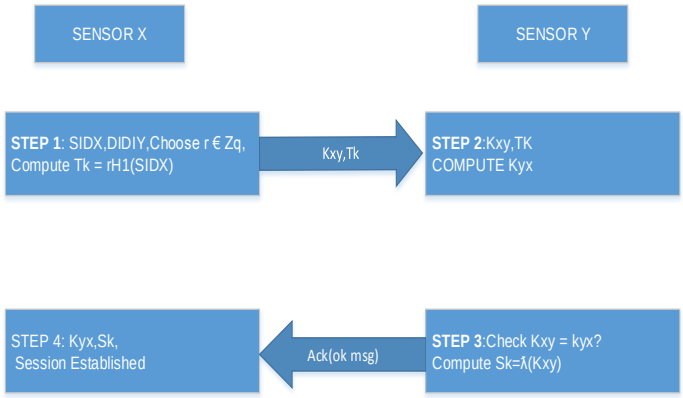

Fig. 2: Pictorial representation of steps for Session Establishment

B. SECURITY ANALYSIS

To evaluate the security of the proposed protocol SET-CRA, we have analyzed various range of security attacks and the protocol can provide strong defense against various adversaries and attacks.

4.2.1 Node Compromising Attacks

Such attacks and attackers are considered as the most

threaten adversaries. Such attackers can access the secret information stored in the compromised nodes, e.g., private or public keys, session keys, node identities etc.

4.2.2 Passive Attacks

Attacks like eaves dropping, traffic congestion can be initiated during anytime of the wireless network deployment. Such passive attackers can also monitor the network and can prepare themselves for carrying-out future attacks.

4.2.3 Active Attacks/Real-time Attacks

Active attackers have greater ability than passive adversaries, which can tamper with the active wireless channels. Therefore, the attackers can forge, reply and modify messages. Nowadays in WSNs, attackers have started implementing numerous active attacks like bogus and replayed routing attacks, node-capture attack, cloning attack etc.

V. EXPERIMENTS AND RESULTS

The various experiments has been done by using Tossim Simulators and tested on numbers of sensor nodes as shown in following figures. The matrix used for experiment results are Energy consumption, First node dies time (FND time), Last node dies Time (LND time) and number of Alive Nodes as describes below:

A. Message Size Analysis

Message size for the transmission is very essential parameters as it regulates the calculation workload and efficiency of the protocol. Table 2 represents message size evaluation of proposed protocol SET-CRA and Table 3 represents different parameters of TinyOS which have been used at the time of implementation. Detailed comparisons are shown in Fig.3

Table 2: Message Size Evaluation

Sr. No.	Parameters	Description	Size(bytes/bits)
1	$SIDX_p$ (p is transmitted packet)	Node identity of transmitted packet p	2 bytes
2	R	Message Size	10- 15 bytes
3	Key size	RSA	1024 bits
4	V	Variable	Approx. bytes

Table 3: TinyOS Parameters

Sr. No.	Parameter	Size
1	Max. message size	35-40 bytes
2	Radio Date Rate	19.2 kbps
3	Power Out	0 db/mv
4	Duty Cycle	100%

B. FND Analysis

FND time describes the duration when first node in wireless sensor network dies. It is essential as this simulation time prompt the commenced worst of the deployed wireless sensory networks represents in Fig. 4

C. LND Analysis

This represents when the whole sensor network becomes idle or when all the sensor nodes will turn sluggish. In Fig. 5, proposed protocol has been evaluated with the other authoritative energy efficient protocols.

D. Number of Alive Nodes

Wireless sensor network have capability of sensing the environment and gathering data from one or more trusted gateways. These entire things depend on the sensing ability of alive nodes in a network. Here theoretical and practical analysis has been done and identified alive nodes of SET-CRA protocol and also comparison with the other protocols as shown in Fig. 6

E. Energy Consumption Analysis Using Power Tossim

In wireless sensor network, minimizing the energy consumption workload is as important as providing good security. So here detailed analysis and comparisons of various methodologies have been done as shown in Fig. 7.

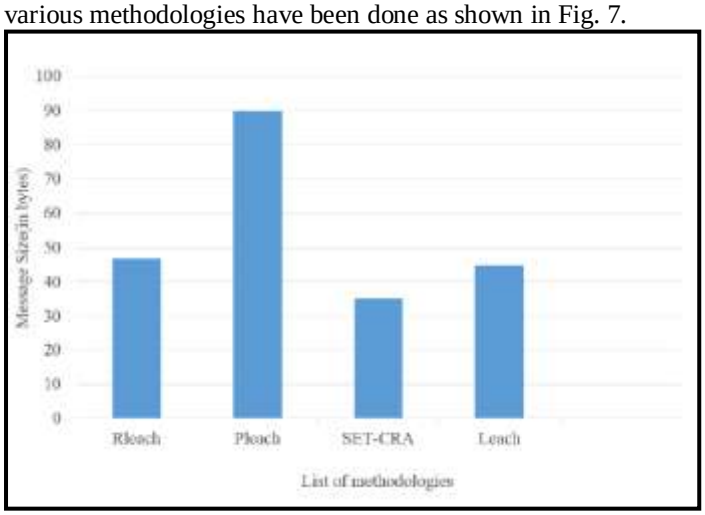

Fig. 3: (Message Size Analysis of SET-CRA with Other Security schemes)

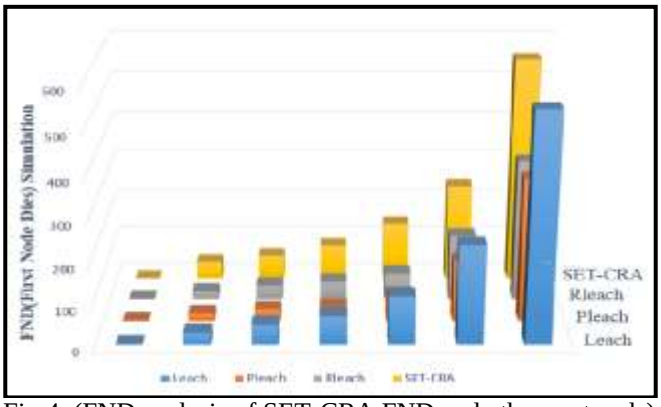

Fig.4: (FND analysis of SET-CRA FND and other protocols)

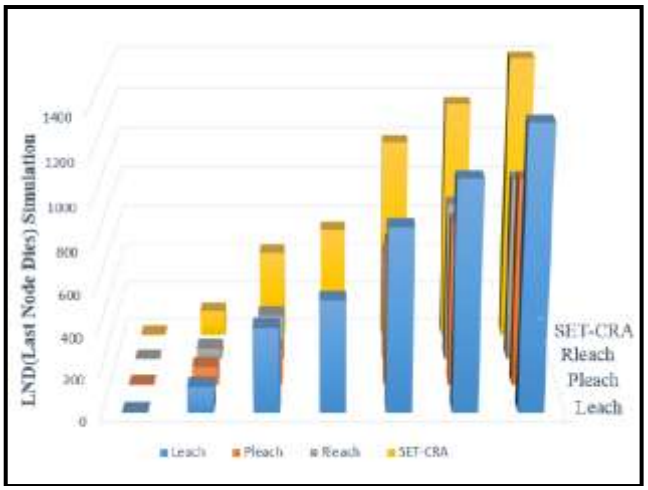

Fig.5: (LND Analysis of SET-CRA and other Security Schemes)

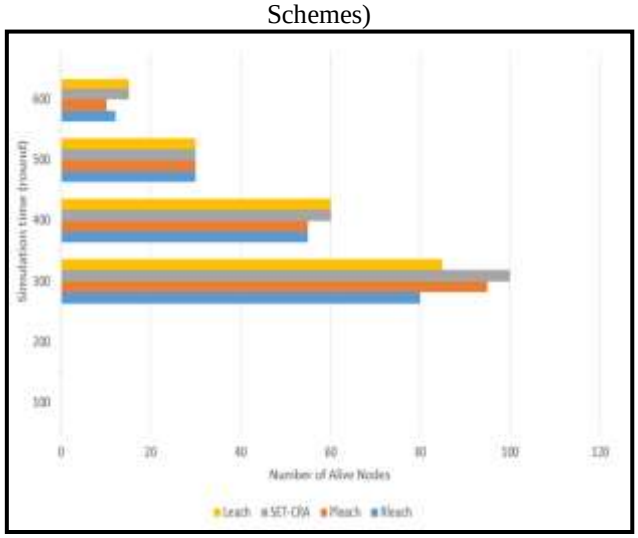

Fig.6: (Numbers of Alive Nodes in SET-CRA in Comparison with other Security Schemes)

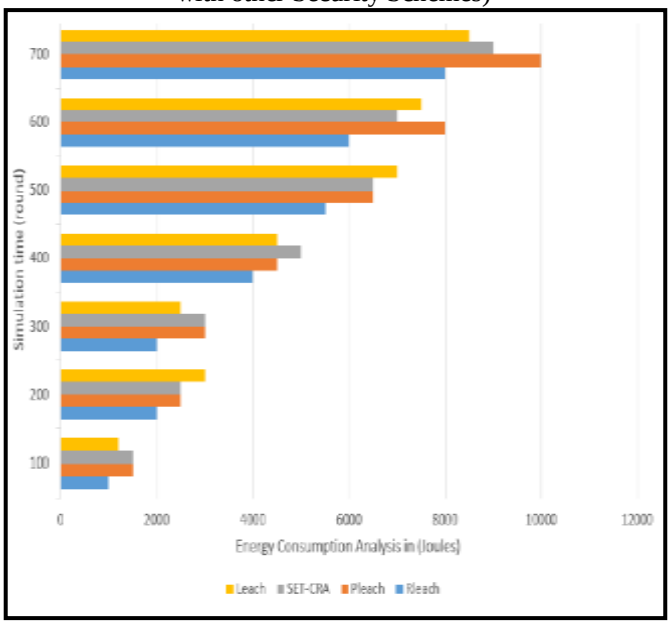

Fig. 7 :(Energy Consumption Analysis of SET-CRA with Other Security schemes)

VI. CONCLUSION

In this paper, it has been traced numerous security challenges, security attacks and analysed various Leach like methodologies in centralized wireless sensor environments. It is then proposed centralized security protocol called "SETCRA", discussed its characteristics, various passive, active and node compromising attacks. In the evaluation section, it has evaluated the proposed "SET-CRA" protocol against numerous security attacks, security methodologies, communication and computation overhead. It has also provided solutions to provide strong defence against wide range of security attacks by using RSA-system authentication scheme and session key establishment scheme. At last but not least, we have compared the proposed protocol with the latest research methodologies in terms of transmitted packet size, FND time, LND time, number of alive nodes and energy consumption. Eventually it is proved that this scheme satisfies high-level security requirements needed in militaries or government organizations.

REFERENCES

[1] Network Management in Wireless Sensor Networks. Winnie Louis Lee, Amitava Datta, and Rachel Cardell-Oliver. School of Computer Science & Software Engineering The University of Western Australia.

[2] Security in Wireless Sensor Networks: Issues and Challenges". Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala. Proceeding of the 2013, IEEE International Conference on Space Science and Communication (IconSpace).

[3] Overview of Security Issues in Wireless Sensor Networks. Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh. 2011, IEEE - Third International Conference on Computational Intelligence, Modelling & Simulation.

[4] Comparison of Security Protocols for Wireless Sensor Networks. Tae Ho Kim, Chang Hoon Kim, Chun Pyo Hong, and Hiecheol Kim. Dept. Computer and Communication Engineering, Daegu University.

[5] Wireless Sensor Network Security: A Critical Literature Review. Alexander Betts, Frank Meyer-Bodemann, Fred Muller and Shao Ying Zhu. October 21-23, 2013, IEEE-COMCAS, pp. 1-5.

[6] Wireless Sensor Network: Security challenges. Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI. April 20-21, 2012, Proceedings of National Days of Network Security and Systems (JNS2), pp. 68-72.

[7] Security Frameworks for Wireless Sensor Networks-Review. Gaurav Sharma, Suman Balaa, Anil K. Verma. 2012, Procedia Technology, 2nd International Conference on Communication, Computing & Security [ICCCS], Vol. 6, pp. 978-987.

[8] Secure and Efficient Data Transmission for

Cluster-Based Wireless Sensor Networks. Huang Lu, Jie Li and Mohsen Guizani. 3, MARCH-2014, IEEE-TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Vol. 25, pp. 750-761.

[9] CENTER: A Centralized Trust-Based Efficient Routing Protocol for Wireless Sensor Networks. Chehab, Ayman Tajeddine Ayman Kayssi Ali. Paris : s.n., July 16-18, 2012, Proceedings of Tenth Annual International Conference on Privacy, Security and Trust, pp. 195-202.

[10] Centralized Key Management Scheme in Wireless Sensor Networks. Saber Banihashemian, Abbas Ghaemi Bafghi ,Mohammad Hossien Yaghmaee Moghaddam. 3, 27 April 2011, Wireless Personal Communications, Vol. 60, pp. 463-474.

[11] An Enhanced and Secured RSA Key Generation scheme (ESRKGS). M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya. 2014, Journal of Information Security and Applications, Vol. 20, pp. 3-10.

[12] PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks System. Sangho Yi, Junyoung Heo , Yookun Cho , Jiman Hong. 14-15, 2007, Computer Communications, Vol. 30, pp. 2842-2852.

[13] SecLEACH—On the security of clustered sensor networks. Leonardo B. Oliveiraa, _, Adrian Ferreirac, Marco A. Vilac-ac, Hao Chi Wongb, Marshall Bernb, Ricardo Dahaba, Antonio A.F. Loureiroc. 12, 2007, SIGNAL PROCESSING-ELSEVIER, Vol. 87, pp. 2882-2895.

[14] Recent advances and future trends in Wireless Sensor Networks. Vivek Katiyar, Narottam Chand, Naveen Chauhan. 3, 2010, International Journal of Applied Engineering Research, Vol. 1, pp. 330-342.

[15] WIRELESS SENSOR NETWORK SECURITY THREATS. Gurudatt Kulkarni, Rupali Shelk , Kiran Gaikwad, Vikas Solanke , Sangita Gujar , Prasad Khatawkar. s.l. : IET Conference Publications, 2013, Proceedings of Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom).

