A Comparative Study for Source Privacy Preserving and Message Authentication in Wireless Sensor Networks

Mr. Harish. G
Department of C.S.E,
Dr. A.I.T, India

Mrs. Smitha Shekar. B
Department of C.S.E,
Dr. A.I.T, India

Ms. Geetha. P. L
Department of C.S.E,
Dr. A.I.T, India

Abstract - Source node privacy and message authentication are the most important issues to be addressed in wireless sensor networks. Many schemes have come up to deal with message authentication. However, some of the schemes have stood by with some limitations like lack of scalability and high communication and computational overhead. Later these issues were solved by a polynomial based scheme, but failed to transmit number of messages beyond its threshold. To overcome this limitation an ECC and RSA algorithm has been used. To fix all these issues, a source node privacy based message authentication using Greedy Random walk algorithm has been proposed in this paper. A comparative study is done for the work that is implemented using ns2 and matlab.

Keywords: **Wireless** ***Sensor Networks (WSN), Greedy Random Walk (GRW), Source Privacy, Message Authentication***

I. INTRODUCTION

A remote sensor system (WSN) comprises of spatially circulated self-governing sensors to screen physical or ecological conditions, for example, temperature, sound, weight, and so forth and to agreeably go their information through the system to a principle area. The more cutting edge systems are bi-directional, additionally empowering control of sensor action. The advancement of remote sensor systems was roused by military applications, for example, war zone reconnaissance; today such systems are utilized as a part of numerous mechanical and purchaser applications, for example, modern procedure observing and control, machine wellbeing checking, etc. Wireless Sensor Networks (WSN) is the collection of autonomous sensors that are spatially distributed. The sensor nodes responsibility is to monitor environmental or physical conditions like pressure, temperature, etc., and to synchronically transfer their data through the network. In that case, the most important point of concern will be the authentication of the messages transferred and the privacy of the source node that transfers the messages to other node.

Message Authentication hinders the transmission of illegal and corrupted messages in the wireless sensor networks. As a result many message authentication schemes were developed to achieve message Authenticity based on public-key and private-key cryptosystems which led to complex key management, lack of scalability and high overhead. To acknowledge these issues a polynomial-based scheme was introduced but it failed when the member of messages transmitted exceeded its threshold limit. This issue can be overcome in Elliptic Curve Cryptography (ECC) method and also RSA algorithm. Source node privacy is also one of the important issues. In spite of strong encryption, there are chances of data getting exposed in wireless sensor network. The data can be any kind of identity information of a particular node. In this paper, a source node privacy based message authentication using ECC and Greedy Random Walk (GRW) algorithm to enable source privacy has been proposed. A comparative study is provided in two different platforms, i.e., matlab and ns2.

II. LITERATURE SURVEY

In the paper titled Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks [1], Jian Li, Yun Li, Jian Ren and Jie Wu proposed an efficient and scalable message authentication scheme based on ECC and hop-by-hop message authentication, to overcome high overhead and to provide message source privacy. In the paper titled Preserving source location privacy in monitoring-based wireless sensor networks [2], Yong Xi, Loren Schwiebert and Weisong Shi proposed a two-way random walk algorithm to reduce an eaves dropper from collecting the information. The delivery rate is improved by greedy forwarding and local broadcasting.

In the paper titled Random Walk Routing in Wireless Sensor Networks [3], Milad Kharratzadeh has presented a review on routing techniques in wireless sensor networks, based on random walk applied to different kinds of topologies like regular and random topologies.In the paper titled An Effective Scheme of Location Privacy Preserving in Monitoring system for WSNs [4], K. Chaitanya Jyoti and V. Srinivas proposed a verification of privacy protection under backtracking attack model and also the analysis of energy consumption. In the paper titled Protecting Location Privacy in Wireless Sensor Networks against a Local Eavesdropper-A Survey [5], Chinnu George and Dhinakaran Nathaniel presents a survey on existing privacy techniques in wireless sensor networks. They explained scenario of panda-hunter problem with respect to the location privacy.There are chances of losing location information causing to suppress the entire network.

In the paper titled Source Location Privacy considerations in Wireless Sensor Networks [6], Ruben Rios and Javier Lopez have given a survey regarding solutions to the threats especially in maintaining the privacy in wireless sensor networks. A wireless sensor network consists of the sensors embedded in the environment which are responsible for monitoring certain conditions. In such cases there are chances of privacy getting tampered. In the paper titled Emulated Source/Sink Location Privacy Algorithm [ESLPA] for Secure Node and Sink in WSN [7], D. Gopinath and P. Ramesh propose an ESLPA algorithm to address the data security and location privacy and to improve node level and sink level privacy. It also deals with the source anonymity problem. In the paper titled Protecting Location Privacy in Wireless Sensor Networks against Eavesdropper [8], Seema Goswami, Prof. Nidhi Chandrakar, Prof. Somesh Dewangam propose a greedy random walk mechanism to deal with the source location privacy protection in wireless sensor networks since sensor nodes are always at risk of its data and information getting exposed. In the paper titled Using MD5 and RSA Algorithm Improve Security in MANETs Systems [9], Karamjeet Singh and Chaksher Goel propose a combination of MD5 and RSA approaches to protect the data from various kinds of attacks. In the paper titled Secure Attribute Based Disruption Tolerant Military Networks [10], Ms. Selva Sangeetha. S, Ms. Sharmila. S and Ms. Kalaivani. M propose a secure attribute based scheme using rsa algorithm when there is no direct connection between the source and the destination.

III. RELATED WORK

Message authentication and source node privacy are important issues in wireless sensor networks. Many techniques have been proposed such as polynomial-based schemes random walk [3], location privacy [4] to address certain issues like limiting the number of messages to be transmitted. But these techniques also leave behind certain issues that need to be addressed. Privacy means protecting the data related to source like its ID and location. Many such privacy techniques have been designed in wireless sensor networks. The privacy techniques in wireless sensor networks can be classified as shown in the Fig. 1.

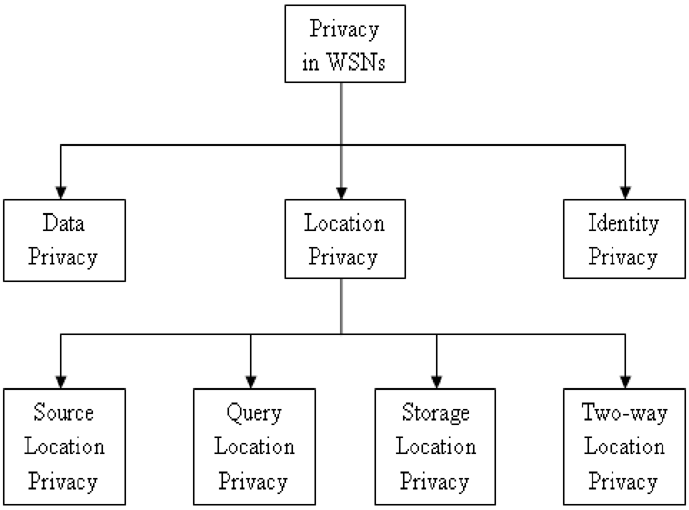


Fig. 1: Taxonomy of privacy techniques in WSNs

IV. PROPOSED SYSTEM

Here there is an attempt to build a source node privacy protection using Greedy Random walk (GRW) algorithm. The flow of the proposed system is shown in the Fig. 2.

The proposed system targets at attaining the following goals:

Message Authentication: Each message receiving node should verify whether the message at the receiving end is sent from the claimed user which is achieved using ECC.

Source identity and location privacy: Sender's information like sender's ID and location information cannot be determined by the rival. To achieve this Greedy Random Walk algorithm is implemented.

A. Message Authentication

*1) **ECC algorithm:*** In this project, the Scalable Message Authentication scheme is proposed for secure message sending. The proposed scheme allows any node to transmit an unlimited number of messages without suffering from threshold problem. We are using ECC signature for message authentication. This scheme enables the nodes to authenticate the message so that all corrupted message can be detected and dropped.

2) The ECC encryption and signature generation is demonstrated below. Consider the parameters required for the ECC algorithm which can be p (prime number), a & b (integer coefficients), G (base point), n (order of the curve generator G), h (cofactor)

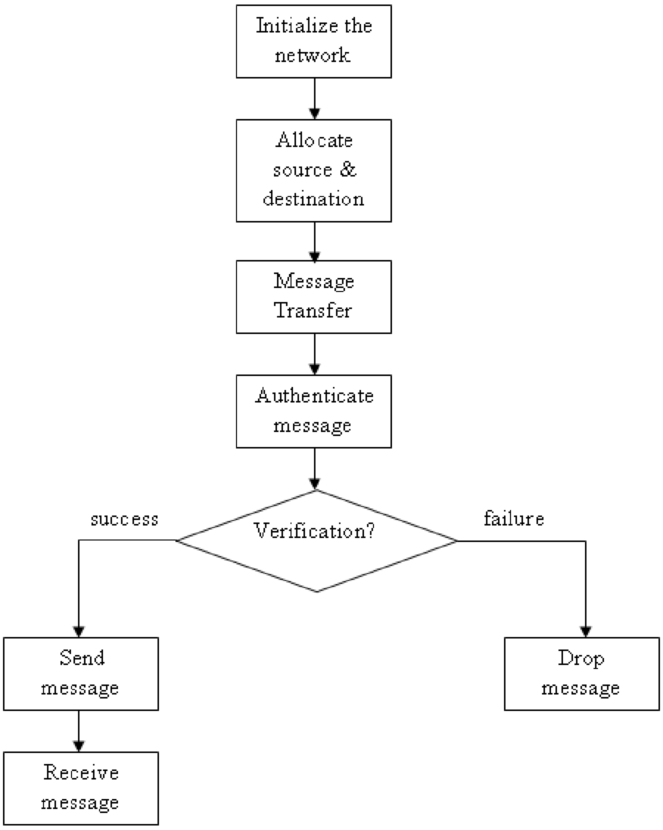


Fig. 2: Flowchart of the proposed system

Key Generation

Choose a random integer d to get the private key such that 0 < d < n
Then compute the public key P = s * G

Encryption

Choose a random integer r such that 0 < r < n
Calculate point R as a product of r and G, R = r * G
Ciphertext = r * G, m + r * P

Signature Generation

Select the parameters q, s, a, b, P, N, h
Let d be the private key and m be the message
Select random integer k and perform scalar multiplication i.e., k * p
Compute the hash function e = H(m)
Compute S = k^{-1} (e + d r) mod n
The signature of message m is (r,s)

Signature verification

Compute the hash function e = H(m)
Compute w = S^{-1} mod n

u_1 = ew mod n and u_2 = rw mod n
x = $u_1P + u_2Q = (x_1 , y_1)$
v = x_1 mod n

verify whether v = r. if so then signature is verified.

3) **RSA algorithm:** In this paper, encryption and authentication have been proposed in order to attain confidentiality and integrity using RSA algorithm.

Key Generation

Initially encryption is achieved for a message M sent by the source, by choosing two prime numbers p and q. Then $\phi(n)$ is computed as a product of (p -1) and (q – 1),

$$\phi(n) = (p - 1)(q - 1)$$

The value of e is chosen and the value of d is computed using,

$$d\,e \equiv 1 \ (\bmod\ \phi(n))$$

The public key pair will be (e , n) and the private key pair will be (d , n).

Encryption and Decryption

Suppose m is the message that the source wishes to send. It is encrypted using the public key pair which results as a cipher text.

$$C = M^e \bmod n$$

The cipher text is sent to the destination through the set of nodes in the path to the destination, where the receiver decrypts the cipher text using the private key pair that results with the original message.

$$M = C^d \bmod n$$

Signature Generation

RSA also promotes authentication of the message by attaching the signature to the message. The source can use its own private key to generate a signature.

$$S = M^d \bmod n$$

Signature verification

The signature is attached to the message and sent to the nodes and also the destination where they verify the signature using the public key.

$$M' = S^e \bmod n$$

Each node verifies the signature assuring that the message has arrived from a valid node.

B. *Source Node Privacy*

In order to increase the source node privacy protection, Greedy Random Walk (GRW) technique has been proposed. There are chances of adversary knowing the source information like its ID and location. To address these issues Random Walk was developed. The basic idea of random walk is that each packet takes a different path to the sink node and it does not disclose any data about the source. A Greedy Random Walk (GRW) also termed as two-way random walk reduces the chance of an illegal user collecting source related information. They use local broadcasting and greedy forwarding to improve the delivery rate. The sink node sets up a path using random walk that consists of nodes called as receptors which are as shown in Fig. 3a. Each packet is forwarded to the sink node from the source until it reaches one of the receptors and then forwards the packet to the sink node through the pre-established path as shown in the Fig. 3b. The greedy random walk chooses the path in a greedy manner. Each time the sensor picks up one of the neighbors randomly that is not recently visited. It always tries to choose an unvisited area.

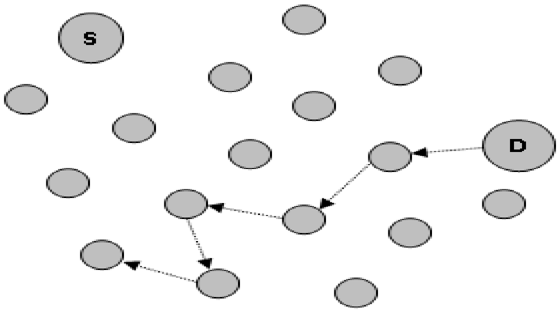


Fig. 3a: Random walk mechanism

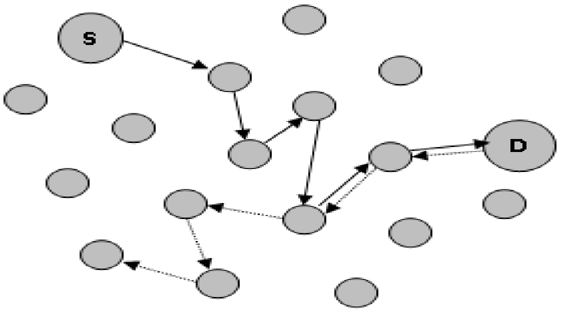


Fig. 3b: Greedy walk mechanism

V. EXPERIMENTAL SETUP

A. *NS2*

This project is implemented using ns2 simulator. The Fig. 4 gives the picture of deployment of the nodes in which 40 nodes are deployed in the network among which source and is selected by the user and destination node is fixed. The user can select the message for transmission from source to destination through receptor nodes. The greedy random walk algorithm is used for selecting the path from source to destination.

Once the path is selected the message which has to be transferred will be encrypted and forwarded to the nodes in the path, where each and every node are going to authenticate whether the data is corrupted or not which is shown in Fig. 5. If data is corrupted the packet will be dropped else data will be transferred to destination successfully.

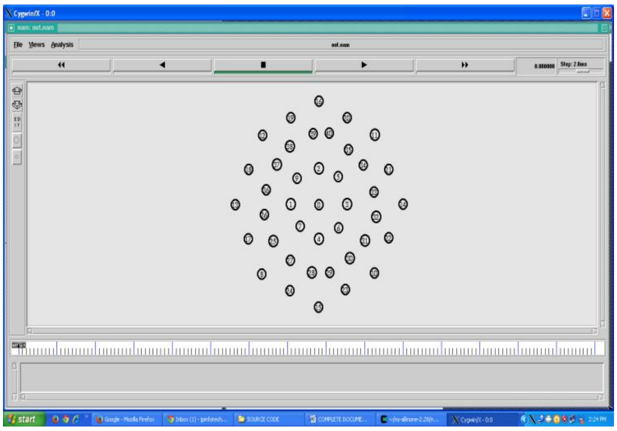
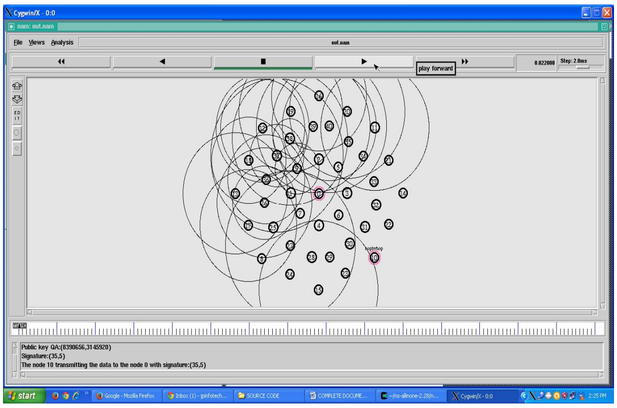


Fig. 4: Deployment of nodes



Public key QA:(8390656,3145920)
Signature:(35,5)
The node 10 transmitting the data to the node 0 with signature:(35,5)

Fig. 5: Transmission of data

B. MATLAB

This project is also implemented in matlab where we deploy 30 nodes in an X-Y plane. The deployment of nodes in matlab is shown in the Fig. 6. The nodes are scattered randomly in the defined field. The key distribution for the nodes is depicted in the Fig. 7 and the transmission of packets between source and destination through the receptor node is shown in the Fig. 8.

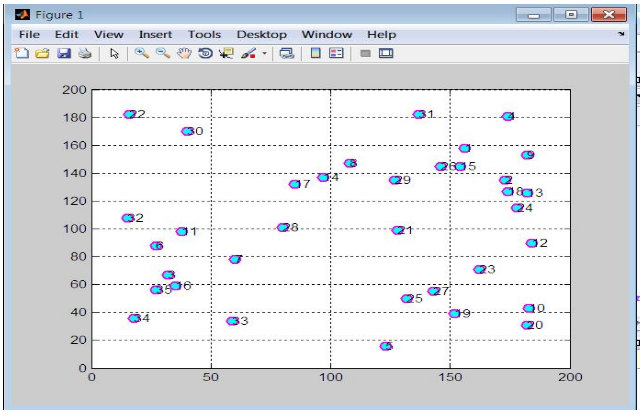


Fig. 6: Node Deployment

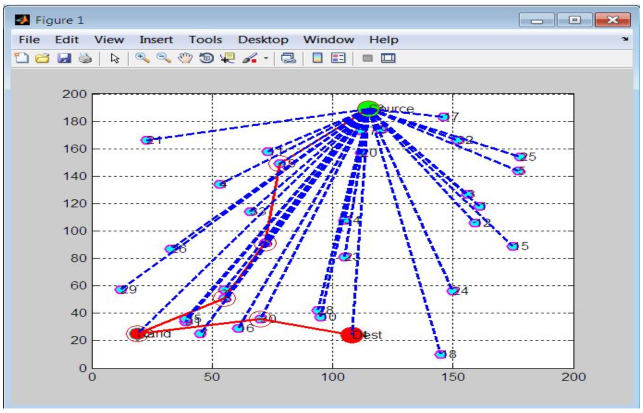


Fig. 7: RSA key distribution

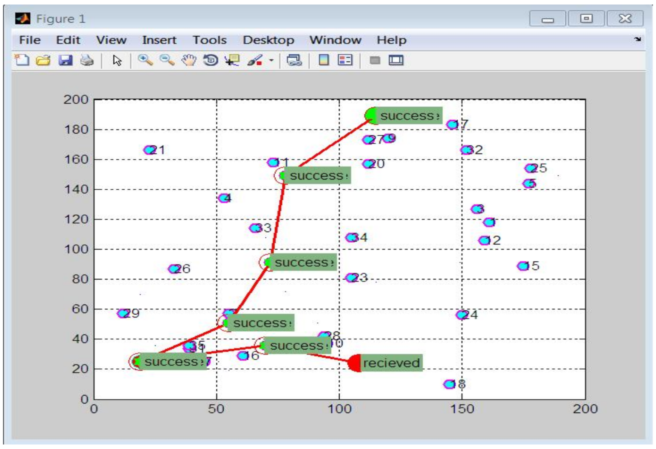


Fig. 8: Transmission of packets

VI. RESULTS

This section is going to give the overview of the performance measurement of the system in ns2 and matlab. The Fig. 9 shows the graph which clearly tells us the packet delivery ratio for ECC and Fig. 10 depicts the energy consumption for Greedy Random Walk implemented in ns2.

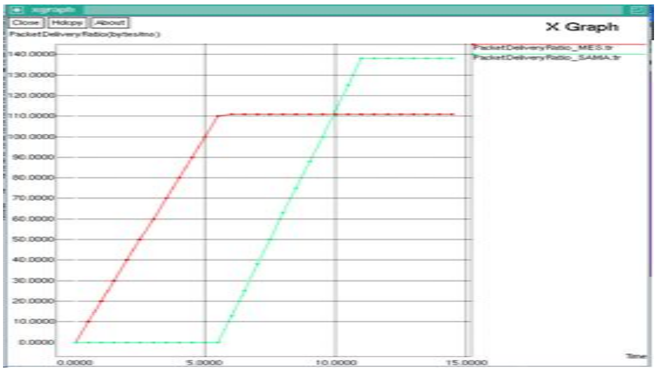


Fig. 9: Results showing packet delivery ratio in ns2

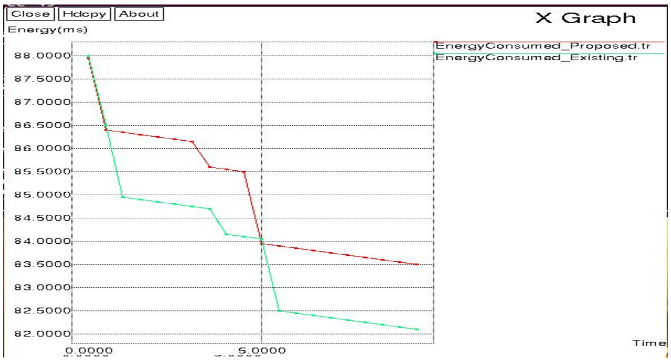


Fig. 10: Results showing the energy consumption in matlab

The packet delivery ration of our system is better than the existing system because of the use of the greedy random walk algorithm which takes less time for transferring packets from source to destination. And Fig. 11 shows the energy consumption for Greedy Random Walk implemented in matlab.

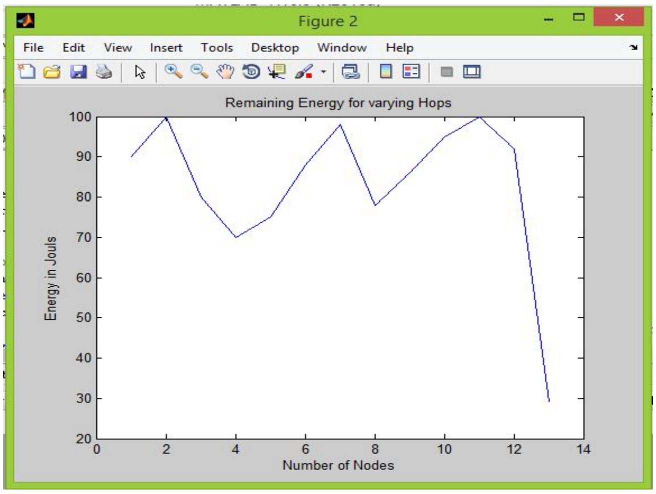


Fig. 11: Results showing the energy consumption in matlab

We can infer from the results that the values of ns2 are comparatively more accurate than that of matlab.

VII. CONCLUSION

In this paper, first a novel and efficient RSA algorithm has been proposed in matlab and a scalable ECC authentication is implemented in ns2 to ensure the confidentiality and integrity of the messages and providing a comparative study. While ensuring message sender privacy, Message Authentication can be applied to any message to provide message content authenticity using ECC and also in RSA. To preserve the source privacy, Greedy Random Walk method for routing the data from source to destination has been designed which improves the performance of the system. Energy consumption is also reduced when compared to other routing algorithms. The random walk is a considerable approach for source privacy.

REFERENCES

[1] Jian Li, Yun Li, Jian Ren, Jie Wu, "*Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks*", Volume 25, No. 5, May 2014.
[2] Yong Xi, Loren Schwiebert, and Weisong Shi, "*Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks*".
[3] Milad Kharratzadeh, "*Random Walk Routing in Wireless Sensor Networks*".
[4] K. Chaithanya Jyothi and V. Srinivas, "*An Effective Scheme Of Location Privacy Preserving In Monitoring System For WSNs*", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.
[5] Chinnu George and Dhinakaran Nathaniel, "*Protecting Location Privacy in Wireless Sensor Networks against a Local Eavesdropper-A Survey*", Volume 56, No. 5, October 2012.
[6] Ruben Rios, Javier Lopez, "Source *Location Privacy considerations in Wireless Sensor Networks*".
[7] D. Gopinath, P. Ramesh, "*Emulated Source/Sink Location Privacy Algorithm [ESLPA] for Secure Node and Sink in WSN*", Vol. 3, Issue 12, December 2015.
[8] Seema Goswami, Prof. Nidhi Chandrakar, Prof. Somesh Dewangam, "*Protecting Location Privacy in Wireless Sensor Networks against Eavesdropper*", Vol. 3 Issue 3, March 2014.
[9] Karamjeet Singh, Chaksher Goel, "*Using MD5 and RSA Algorithm Improve Security in MANETs Systems*", Vol 2 Issue 2, June 2014.
[10] Ms. Selva Sangeetha S, Ms. Sharmila S, Ms. Kalaivani M, "*Secure Attribute Based Disruption Tolerant Military Networks*", Volume 3, Issue III, March 2015.
[11] Pallavi S. Patil, Jyoti N. Nandimath, "*A Survey Paper on Scalable & Routing Efficient Methods for Source Location Privacy in WSNs*", Vol. 3 Issue 2, February 2014.
[12] Young Sil Lee, Esko Alasaarela, Hoon Jae Lee, "*An Efficient Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System*", Vol. 8, No. 3, 2014.
[13] H. Wang, S. Sheng, C. Tan, and Q. Li, "*Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control*", IEEE ICDCS, Beijing, China, 2008.
[14] Aqeel Khalique, Kuldip Singh, Sandeep Sood, "*Implementation of Elliptic Curve Digital Signature Algorithm*", Vol 2 – No 2, May 2016.
[15] Karamjeet Singh, Chakshu Goel, "*Using MD5 and RSA Algorithm Improve Security in MANETs Systems*", Vol 2, Issue 2, June 2014.

[16] Ms. Selva Sangeetha S, Ms. Sharmila S, Ms. Kalaivani M, "*Secure Attribute Based Disruption – Tolerant Military Networks*".

[17] J. Jeyasoundari, M. Monisha Devi, M. Saranya, "*Efficient Authentication Scheme for Multicasting over Ad-hoc Networks*", Volume 3, Issue 11, November 2013.

[18] Yun Li, Jian Ren, "*Preserving Source – Location Privacy in Wireless Sensor Networks*", 2009 IEEE.