www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 10 October, 2014 Page No.8865-8870

Implementation on Secure Routing Method for Detecting False Reports and Gray-hole Attacks along with Elliptic Curve Cryptography in Wireless Sensor Network

Ms. Sneha M. Sakharkar [1], Prof. R. S. Mangrulkar [2]
Dept. of Computers Engineering
Bapurao Deshmukh College of
Engineering, Sevagram, India
snehasakharkar@gmail.com[1], rsmangrlkar@gmail.com[2]

Abstract- Wireless Sensor Networks (WSNs) are used in many applications in military, environmental, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this paper, we explore security issue in WSN. First, the constraints, security requirements and attacks with their corresponding countermeasures in WSNs are implemented. Individual sensor nodes are subject to compromised security. An adversary can inject false reports into the networks via compromised nodes. Furthermore, an adversary can create a Gray hole by compromised nodes. If these two kinds of attacks occur simultaneously in a network, some of the existing methods fail to defend against those attacks. The Ad-hoc On Demand Distance (AODV) Vector scheme for detecting Gray-Hole attack and Statistical En-Route Filtering is used for detecting false report. For increasing security level, the Elliptic Curve Cryptography (ECC) algorithm is used. Simulations results obtain so far reduces energy consumption and also provide greater network security to some extent.

Keywords- Wireless Sensor Network, Gray-Hole Attack, False Report, Elliptic Curve Cryptography..

1. INTRODUCTION

A WSN consists of a large number of sensor nodes that monitor the environment and one or more base stations collect the sensor readings.[1],[2],[3],[4],[5] In many applications such as military surveillance, sensor nodes are deployed in open, large-scale, and even hostile environments and potential issues range from accidental node failure to intentional tampering. Due to their relatively small sizes and unattended operations, sensor nodes are at high risk of being physically captured and having their security compromised. Additionally, the power of the sensor nodes is limited and non-replaceable. The security and energy efficiency of sensor nodes are extremely important in WSNs.[6][7][8]

If sensor nodes are physically captured and compromised, security information such as network keys can be revealed to the adversary.[9],[10],[11],[12] The adversary can then inject false reports into sensor network via the compromised nodes. These injected false reports can not only result in false alarms but also in quick usage of the limited amount of energy in the sensor nodes. Several researchers have proposed mechanisms to combat attack by injection of false reports. The method statistical enrouting filtering method is used to detect and drop injected false reports during the forwarding process[13],[14],[15],[16].

Another type of wireless sensor network attack is a Gray Hole attack [17],[18],[19],[20]The AODV routing protocol is an on-demand routing protocol . Only when two nodes need for communication and the source node does not have route to the destination, in the own routing table. The route request (RREQ) is broadcasted in the network and the destination or intermediate node having route entry in the destination in the routing table will send route reply(RREP) to the original source. The RREQ and RREP process.[21],[22],[23]

Security issues in wireless sensor network can be broadly classified into categories: cryptography, key management, secure routing, etc [24],[25],[26],[27],[28]For more security in the wireless sensor network the Diffie-Hellman methods and Digital Elliptic Curves is used over finite field .Public key systems are secured by assume that it is difficult to factor a huge integer composed of two or more huge prime factors. The curve based protocol, suppose for finding the prime number, the arithmetical operation is used to identify using elliptic curve as, $\beta 2 = \alpha 3 + P\alpha + Q$, where $4P3 + 27Q2 \neq 0$ and for value of P and Q gives (α,β) which satisfies the time without end lies on the curves[29][30] and above equation also. The ECC is performed on both the pair of key, public and private key[20][21]. When private key is multiplied with generated point 'G', the public key is obtained.[31],[32],[33],[34]

2. OBJECTIVES

2.1. Detecting of Attack

Multiple attacks in wireless sensor network, particularly false report injection and gray-hole attack has focused at same time. This false report injected by using compromised node into

network. It can be detected by using Statistical En-route Filtering. The another attack is gray hole attack, For detecting these attack the AODV Protocol is used when forwarding the data. Hence, simultaneously two attacks are detected.

2.2. Security

In wireless sensor network, secure Communication is important. For security Elliptic Curve Cryptography Algorithm (ECC)is used , ECC offers equivalent security level with smaller key size, faster computing with low power and memory consumption and saving in bandwith.ECC is a public key cryptography, where each user or the device taking part in the communication, generally have a pair of key, a public key and private key. The set of operation associated with the key and a set of operation knows the private key, where as the public key is distributed to all users taking part in communication. In insecure channel without exchanging a secrete key the public key cryptography is used and provide a secure communication over a channel.

3.IMPLEMENTED WORK

There are various threats in the wireless sensor network. A false report injection attack shown in Fig1.A compromised node can inject false report into network which wastes the residual energy of the node which deliver them to the base station and lead to false alarms. The detection of false report a statistical en-route filtering method is used .It involves two primary phases: Key assignment report generation and En-Route Filtering. The Base Station (BS) maintains a global key pool and divides it into ‘n’ partitions. Each partition has ‘m’ keys, and each key has a unique key index. User randomly selects ‘k’ key from one partition before nodes are deployed. The selected keys and the associated key indices are stored in the node before being deployed to the sensing field. When an event occurs in the sensing field, all surrounding nodes detect the event, The SEF can detect false reports en-route, detected nodes generate a message authentication code. Cluster head collect the information from the entire node and gives it to the base station, then checks the number of Message Authentication Code (MAC) in the report. If the report has a different number of MAC then the nodes drop the report. Hence Base station is able to verify every MAC because it has all the keys .If there are any mismatches, the base station discard the report.

The Gray Hole attack is one of the network layer attack describe in multihop WSN, the nodes send packets to the neighbouring nodes thinking that they can forward message to the destination faithfully. In gray-hole attack, a malicious or compromised node refuses some packets and drops them. A simple form of this attack is, when malicious nodes act like a black hole and drop all the packet passing through it. A Gray Hole may exhibit its malicious behaviour in various techniques. It drops packets coming from particular nodes in the network while forwarding the packets for other nodes. For some particular time duration malicious nodes can be drop the packets and later may switch to normal behaviour at same time. The combination of above two behaviour may also exhibit so; detection is very difficult, whereas gray-hole attack drops packets at certain frequencies. Both the attacks consist of two steps: Attacker step- The nodes attack other nodes by falsely sending information in the communication. Invaliding step-The node invades the communication process and drops packets. The simple framework of these attacks is over AODVprotocol.

3.1 Algorithm for Gray-Hole Attack.

SN: -Source Node IN:- Intermediate Node
DN:- Destination Node NHN-: Next Hop Node
FRq:- Further Request FRp:- Further Reply
Reliable Node:- The node through which the SN has routed data
DRI:- Data Routing Information
ID:- Identity of the node

1 .SN broadcasts RREQ
2 .receives RREP
3 .IF (RREP is from DN or a reliable node) {
4. Route data packets (Secure Route)
6 .ELSE {
7 .Do {
8 .Send FRq and ID of IN to NHN
9. Receive FRp, NHN of current NHN, DRI entry
10. NHN's next hop, DRI entry for current IN
11. IF (NHN is a reliable node) {
12. Check IN for Gray hole using DRI entry
13. IF (IN is not a Gray hole)
14. Route data packets (Secure Route)
15 .ELSE {
16. Insecure Route
17. IN is a Gray hole
18 .All the nodes along the reverse path from IN to the node
19. that generated RREP are Gray holes
20. }
21 .}
22 .ELSE
23. Current IN = NHN
24 }
While (IN is NOT a reliable node)
}

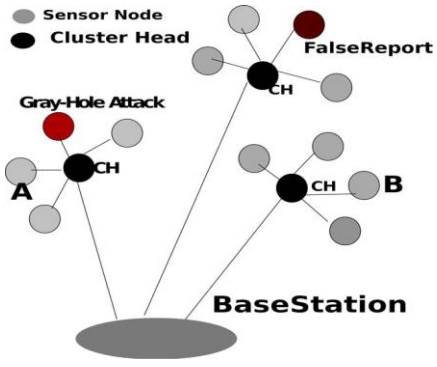

Fig 1. Injection of false Report , Gray-Hole Attack and detecting it.

During the attackers step, the attacker has to identify whether the incoming packets are AODV packets or not then the attacker determines the route and selects the routing by sending RREQ packets. First, the attacker coordinates with routing by simply sending RREQ packets. During Invading step, the attacker starts increasing its sequence number and advertises itself that it has the highest sequence number as

compared to other nodes in the network. Thus, it induces attack by sending a fake reply to the nodes in the network and the data is forged.

Security issues in wireless sensor network can be broadly classified into categories: cryptography, key management, secure routing, etc.

3.2 Key Management:

Key is used for secure communication either in case of symmetric key or asymmetric key algorithms .For implementation of various security scheme Key distribution is not typical in WSNs, but constraints such as small memory capacity make centralized keying techniques impossible. Straight pair wise key sharing between every two nodes in a network is not suitable for large growing networks. A security scheme in WSNs must use efficient and reliable key distribution for secure communication between all relevant nodes.

3.3. Secure Routing:

These protocols are deals with how a node ends message to other nodes or a base station. A major challenge is to verify authentication of the communication broadcast by the base station. Existing methods often uses public key cryptography which has high computational overhead making them infeasible in WSNs The goal of a secure routing protocol is to ensure the integrity, authentication, and availability of messages.

The idea of using Elliptic curves in cryptography was introduced by Victor Miller and N. Koblitz as an alternative to established public-key systems such as DSA and RSA. The Elliptical curve algorithm makes it difficult to break an ECC as compared to RSA and DSA where the problems of factorization or the discrete log problem can be solved in sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other competitive systems such as RSA and DSA. This helps in having smaller key size hence faster computations. Hardware implementation of ECC involves tree-layer hierarchical strategy namely finite field arithmetic, point arithmetic and scalar multiplication .

Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements—i.e., that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key.

For current cryptographic purposes, an *elliptic curve* is a plane curve which consists of the points satisfying the equation along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.) This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety. Hence give the security in wireless Sensor Network.

4. Elliptic Curves over prime fields

Elliptic curves are polynomials that define points based on the (simplified) Weierstra equation:

The mathematical operations of ECC is defined over the elliptic curve,

$$y^2 = x^3 + ax + b,$$

Where, $4a^3 + 27b^2 \neq 0$. Each value of the 'a 'and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. The security is based on the difficultly of a different problem, which is called the Elliptic Curve Discrete Logarithm Problem (ECDLP).

4.1. Geometric Addition:-

Let P(x1,y1) and Q(x2,y2) be two points on the elliptic curve E, shown in fig 2. The sum (x3,y3)= P + Q is defined as: First draw a line through P and Q, this line intersects the elliptic curve at a third point. Then the reflection of this point of intersection about x-axis is (x3,y3) which is the sum of the points P and Q.

Let P(x1, y1), Q(x2, y2) € E(K) Where, E be an elliptic curve defined over the field of integers K and P ≠Q. Then P + Q = (x3, y3). Shown in Fig 1.

Where, $\mathbf{X3= (y2-y1/x2-x1)^2 – x1-x2}$

&

$\mathbf{y3= (y2-y1/x2-x1)(x1-x3)- y1}$

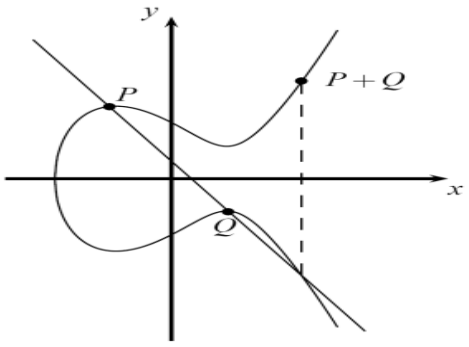

Fig 2. Geometric Point Addition

4.2. Geometric Point Doubling:-

First draw the tangent line to the elliptic curve at P which intersects the curve at a point.Let $P(x1, y1) \in E(K)$ $(a,b)$where P≠ -P then 2P=(x3,y3).Shown in Fig 2.

Where, $\mathbf{X3=(3xi^2 + a/2y1))^2 -2x1}$

$\mathbf{\& \ y3=(3x1^2 + a/2y1)(x1-x3)- y1}$

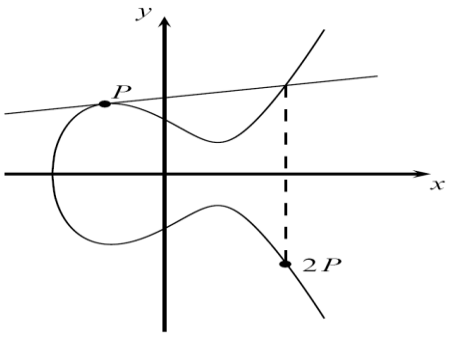

Fig 3.Geometric Doubling Point

4.3. Point Multiplication:-

Let P be any point on the elliptic curve(K). Then the operation multiplication of the point P is defined as repeated addition. kP = P + P +.....k times.

The security is provided by elliptic curve cryptography, When node 'A', communicate with node 'B'; there are various algorithm for detecting number of attacks in communication and provides the security, whereas the public key is distributed to all user taking part in communication. Node 'A' has its own private and public key also node 'B' has its private and public key. When communication is perform then there is no any exchange of a secret key, node 'A' s private key can compare with node 'B's public key then Secrete key is generated. This key is compare with cluster head secrete key if it is same then decrypt the data, otherwise drop the data.

4.4.Steps of Generation of Key pair

1. Global Public Elements. Eq (a, b) elliptic curve with parameters a,b, x & y point on elliptic curve & q be the prime number.

$$Y^2 \bmod q=(X^3+aX+b) \bmod q$$

2. User 'A' Key Generation**,** Select private key kA,E be a point of order n.Where ,kA< n

Calculate public P, P=kA × G

Where, G be the point selected on Elliptic Curve, i.e Generating Point.

3 .User B Key Generation, Select private key kB

Where k B<n

Calculate public M, M=kB × G

4. Generation of Secret Key by user A.

P1=K=kA × M

5. Generation of Secret Key by user B.

P2=K=kB × P

6. The two calculations produce the same result because,

kA × M = kA × (kB × G) = kB × (kA × G) = kB × P

7.To break this scheme ,an attacker would need to be able to compute k given G & kG ,which is found to be tough.

5. SIMULATION RESULT

5.1. Simulation Parameter.

A grid of 1000 x1500 is considered number of nodes: 50.The scenario of communication from one node to other node. The speed for communication as 20m/s with a pause time of 10s. Packet count 10000, transmission time is greater than equal to zero and its statistics shown from node zero to node 49 i. e 50 nodes.

The implementation result broadcast the data and gives the Private and public Key pair using ECC algorithm and communicates from one node to another node.

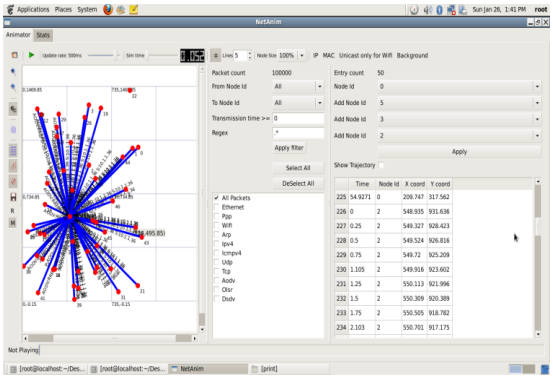

Fig 4. Broadcast the data from one node to other node

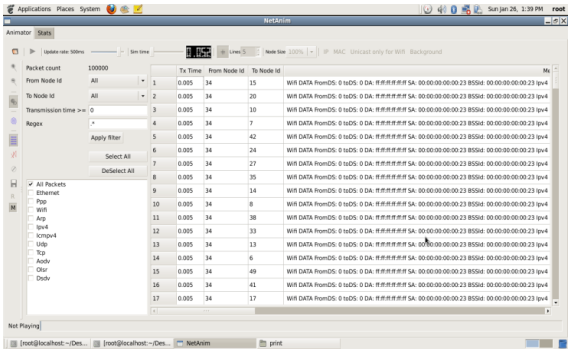

Fig.5 Broadcasting Packet Information

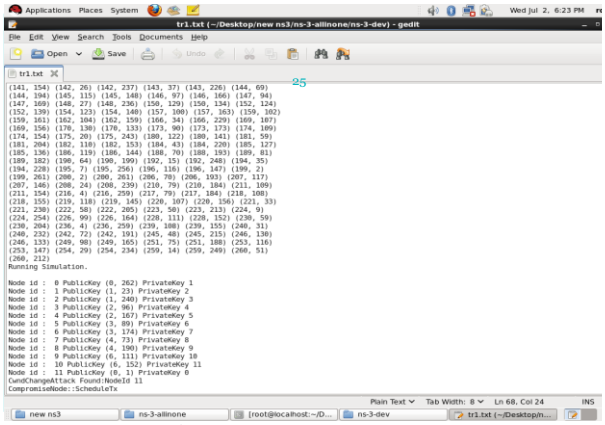

Fig 6 Pair of Key Generation Using ECC Algorithm

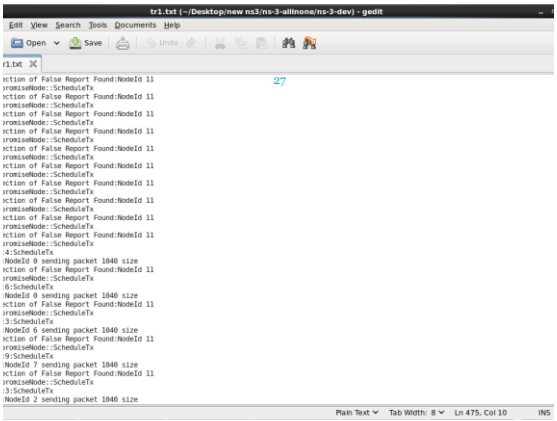

Fig 7.Detecting False Report

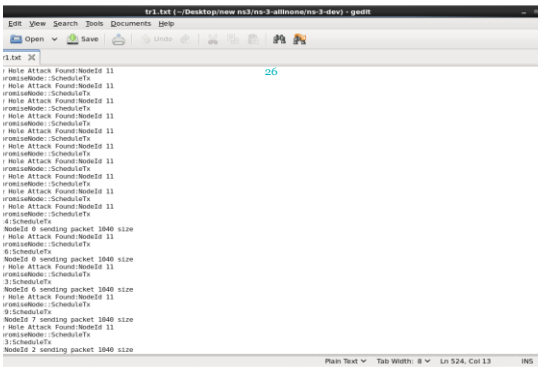

Fig 8. Detecting Gray- Hole Attack

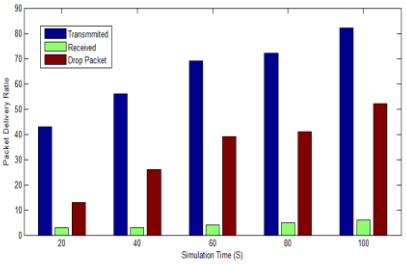

Fig.9. Detecting Packet Drop Ratio.

6. CONCLUSION

We proposed a secure routing method for detecting false reports and Gray-hole attacks in wireless sensor networks.

During literature survey, we found that many of the authors failed to identify security threats and also to provide their countermeasure to overcome those threats. Proposed method perfectly detects false report and Gray-Hole attack using SEF. Proposed methods and to increase the security level. by implementing Elliptical Curve Cryptography which provides more security during data transmission..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 a160-bit elliptic curve key. The advantages can be achieved from smaller key sizes including storage, speed and efficient use of power and bandwidth. The use of shorter keys means lower space requirements for key storage and quicker arithmetic operations. These advantages are essential when public-key cryptography is applied in constrained devices, such as in mobile devices or RFID. In brief, ECC based algorithms can be easily included into existing protocols to get the same backward compatibility and security with smaller resources.

By using this Key Pair, the secure communication establish between two nodes. when communication is establish, then inserted a false report and Gray hole attack between two nodes and these two attack detect it by using suitable algorithm and secure the communication as show in simulation.

/References.

[1] Hyeon Myeong Choi, su man Nam, Tae Ho Cho, *"A Secure Routing for Detecting False Report And Wormhole Attacks In WirelessSensorNetwork",* Lecture Note in Computer Science, Vol. 3420, 2013, pp. 449-458. DOI: 10.1007/978-3-540-31956-6_53.

[2] Alass Atassi, Naoum Saygh, *"Malicious Node Detection in Wireless Sensor Network",* 27th International Conference on Avance Information Networking and Application Workshop, pp. 456-461, 2013.

[3] Al-Sakib Khan Pathan *"Security in Wireless Sensor Networks: Issues and Challenges"* ISBN 89-5519-129-4, pp.1043-1048, Feb.20-22, ICACT 2006.

[4] Usha and Bose, *"Comparing The Impact Of Black Hole And Gray Hole Attack In Mobile Ad-Hoc Network"* Journal of Computer Science 2012, 8 (11), pp. 1788-1802.

[5] Disha G. Kariya, *"Detecting Black And Gray-hole Attack In Mobile Adhoc Network Using An Adaptive Method,"* International Journal of Emerging Technology and advanced Engineering, ISSN 2250-2459,Volume 2,Issue 1, January 2012.

[6] Saranya, M. Usha, S. Jayabharathi, *"An Enhanced Routing Algorithm For Wireless Ad-Hoc Sensor Network"* 5th National Conference; INDIA Com-2011 Computing For Nation Development, March 10 – 11, 2011.

[7] Saranya, M. Usha, S. Jayabharathi, *"An Enhanced Routing Algorithm For Wireless Ad-Hoc Sensor Network"* 5th National Conference; INDIA Com-2011

Computing For Nation Development, March 10 – 11, 2011.

[8] Xiao Zhenghong1, Chen Zhigang, *"A Secure Routing Protocol With Intrusion Detection For Clustering Wireless Sensor Network",* International Forum on Information Technology and Application, pp.-23, 2010.

[9] Su.Man, Sungkyunkwan University,Suwon, Korea, *"Energy Efficient Method for Detection of False Report in Wireless Sensor Network"* pp.766-769,2010-002475 IEEE.

[10] Chun Jin, Xing Liu, Zi Ren, *"Energy-Based Wireless Sensor Networks To Improve The AODV Protocol"*, 978-1-4244-4900-2/09, pp.135-138,2009 IEEE

[11] Giovanni Vigna Sumit Gwalani *"An Intrusion Detection Tool for AODV Based Ad-Hoc Wireless Networks"*, 20th Annual Computer Security Applications Conference (ACSAC_04) 1063-9527/04 IEEE.

[12] Fan Ye.Haiyun Luo, *"Statical En-Route Filtering Of Injected False Data In Sensor Network,"* vol.23,No 4,pp.83 850,April 2005

[13] Theodore Zahariadia and Panagiotis trakades, *"Efficient Detection of Routing Attack in Wireless Sensor Network"* 978-1-4244-4530-1/09 C 2010 IEEE.

[14] R. Poongothai, R. Parthasarthy, *"Performance Analysis of LEACH With Gray-hole Attack In Wireless Sensor Network",* 2012 International Conference on computer communication and informatics 2012-Jan 10- 12, 2012 coimbature, INDIA.

[15] Yin-chun Hu, Carnegie Mellon, *"Packet Leashes: A Defense against Wormhole Attack in Wireless Sensor Network"* 0-7803-7753-2/03 2003 IEEE.

[16] D. Hankerson, A. Menezes, and S.Vanstone, "Guide to Elliptic Curve Cryptography," Springer-Verlag New York, 2004.

[17] P. Kocher, J. Jaffe, and B.Jun, "Differential power analysis,"Proceedings of CRYPTO'99, Springer-Verlag, Berlin, pp. 388–397, 1999.

[18] T.D. Chen, H.Y. Li, K.K. Wu, and F.Q. Yu, "Countermeasure of ECC against Side-channel Attacks: Balanced Point Addition and Point Doubling Operation Procedure," 2009 Asia-Pacific Conference on Information Processing, ShenZhen, vol. 2, pp. 465-469. July 2009.

[19] J. Bringer, H. Chabanne, and T. Icart, "Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters," Applied Cryptography and Network Security, LNCS 6123, 2010, pp. 291–308.

[20] Ms.P.G.Rajeswari, Dr.K.Thilagavathi, "An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009 pp 176-185.

[21] K. Kaabneh and H. Al-Bdour, "Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point", American Journal of Applied Sciences 2 (8): 1232-1235, 2005.

[22] A. Rezai and P. Keshavarzi, " Speed Improvement in elliptic curve cryptosystem scalar multiplication algorithm," proceeding in 7th international ISC conference on information security and cryptology, pp.181-188, Iran, September 2010.

[23] G.M.Dormale and J.J.Quisquater, "High-speed hardware implementations of elliptic curve cryptography: a survey," Journal of systems architecture, vol.53, pp.72-84, 2007.

[24] A. Rezai and P. Keshavarzi, "High-performance Modular Exponentiation Algorithm by Using a New Modified Modular Multiplication Algorithm and Common-Multiplicand-Multiplication Method", in Proceedings of world congress on internet security, in press,2011.

[25] D. Sravana Kumar CH. Suneetha A. Chandrasekhar "Encryption of Data using Elliptic Curve over Finite Fields" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 DOI : 10.5121/ijdps.2012.3125 301

[26] Mrs. Megha Kolhekar,Fr. C. Rodrigues, "Implementation of Elliptic Curve Cryptography on Text and Image" International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849 http://www.ijecbs.com Vol. 1 Issue 2 July 2011.

[27] Felipe Tellez and Jorge Ortiz, "Behavior Elliptic Curve Cryptosystem for the Wormhole Intrusion in MANET" IJCSo.9, Sep 2011.

[28]An Liu; Peng Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on , vol., no.,pp.245-256, 22-24 April 2008.

[29] Yong Wang; Ramamurthy, B.; Xukai Zou; , "The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks," Communications, 2006. ICC '06. IEEE International Conference on , vol.5, no., pp.2243-2248, June 2006.

[30] Standards for Efficient Cryptography Group (SECG), SEC 1: Elliptic Curve Cryptography (http:/ / www. secg.org/ download/ aid-385/ sec1_final. pdf), Version 1.0, September 20, 2000

[31] D. Hankerson, A. Menezes, and S.A. Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag, 2004.

[32] Pierre E. ABI-CHAR, Abdallah MHAMED, *"A Secure Authenticated Key Agreement Protocol Based On Elliptic Curve Cryptography"*, Third International Symposium on Information Assurance and Security, 0-7695-2876-7/07 IEEE.DOI 10.1109/IAS.2007.57, pp.89-94, 2007.

[33] Asha rani Mishra, *"Elliptic Curve Cryptography for Security in Wireless Sensor Network"* IJERT, ISSN: 2278-0181 Vol.1 Issue 3, May-2012.

[34] Felipe Tellez and Jorge Ortiz, *"Behavior Elliptic Curve Cryptosystem for the Wormhole Intrusion in MANET"* IJCSo.9, Sep 2011.