ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

An Enhance Energy Efficient Security in WSN by using Elliptic Curve Session Keys Algorithm

Neha Hans, Neha Goyal[2]

M.Tech Student, Department of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India[1]

Asst. Professor, Department of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India[2]

ABSTRACT: Wireless Sensor Networks (WSNs) are more susceptible to security attacks as compared to wired networks due to their wireless and dynamic behaviour. It is significant to describe whether an incoming message creates from a reliable node or not. The main answer for this is the usage of cryptographically marked messages. Qos and Security is the main issue in wireless sensor network (WSN) because of its wireless communication behaviour and restraints i.e. low computation capability, vulnerability to physical capture or damages, less memory, bounded energy resources and the usage of unprotected wireless communication channels. The cryptographic techniques improve the security level and make it protected against serious attacks but also have an important outcome on the wireless sensor network QoS. In this paper a protected symmetric key will be suggested for WSN. To secure against the attacks appropriate security techniques are needed Elliptic Curve Cryptography (ECC) is the best candidate because of its smaller key size. This thesis concentrates measure and improve the WSN routing protocol performance for monitoring of serious conditions with the help of important metrics i.e. throughput and delay with distinct mechanisms in many scenarios for mobile nodes and then enhance it by our suggested algorithm that depend on Encrypted Session keys. Depending on results obtained from simulation a conclusion is deduced on the evaluation between these different mechanisms with parameters i.e. throughput and delay

KEYWORDS: WSN, ECC, Cryptography, QoS, OPNET

I. INTRODUCTION

One of the most important technologies of this century is Wireless sensor network. For use in remote sensing applications, recent advancement in wireless communications and electronics has enabled the development of low-power, low-cost, multifunctional miniature devices. A sensor network is collection of a great number of sensor nodes which consist of sensing, data communication and processing skill. A unique feature of sensor networks is the cooperative effort of sensor nodes. They use their processing capabilities to locally carry out simple computations and transmit only the needed and moderately processed data, Instead of sending the raw data to the nodes responsible for the fusion. All Sensor networks are data-centric in which sensed data directed to cluster of sensors.

The aggregation of these factors has enhanced the viability of handling a sensor network consisting of a huge number of intelligent sensors, processing analysis, enabling the collection and dissemination of valuable information gathered in a variation of environments. Aggregation of data raises the level of accuracy and decrease data redundancy. A network hierarchy and clustering of sensor nodes allows for network robustness, scalability, lower power consumption and efficient resource utilization. The basic objectives for sensor networks are accuracy, reliability, cost effectiveness, edibility and ease of deployment.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

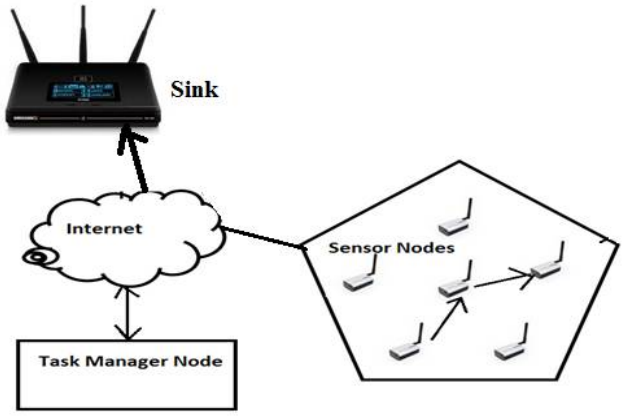

Fig. 1: Wireless sensor Network

II. DESIGN CONSTRAINTS FOR WSNS

Because of the behavior of sensors having decreased computing, battery and radio resources as well as the ad hoc paradigm of wireless sensor networks depending on multi hop to assure connectivity throughout the network without any infrastructure or centralized management any protocol should take into account the following features of a WSN [16, 17, and 18]:

Constrained Devices: Because of their size sensors are highly restricted in resources (battery power, storage capacities, computing power) which builds the applications and protocols development for WSNs a challenging task. Thus the developed protocols and facilities for WSNs must consider these restraints during development by developing effective and robust security or routing protocols by decreasing the no. of operations required for executing any task.

Wireless Medium: Wireless sensor networks utilizes radio waves as transmission medium, inherently susceptible because of its broadcast behavior providing possibility to any intruder with the enough hardware and the network stack to interrupt, eavesdrop or change the transferred data.

The nature of environment: Normally, a wireless sensor networks are targeted for remote controlling and surveillance, deployed in hostile and unpredictable atmosphere, building them subject of several attacks i.e. sensors capture, compromise and spoofing attacks.

High number of sensors: Future wireless sensor networks will have hundreds to thousands of sensors geographically distributed in a huge region, with restricted resources. Thus any developed protocol must permit the network scaling.

Absence of infrastructure: Although a wireless sensor network contains sensor nodes wirelessly connected to one another, responsible of setting up, managing and securing the connectivity with the BS without any administrative authority, hence sensors cooperate in a distributed manner to maintain the network connectivity and security.

III. ATTACKS AGAINST WSN

Because of the behavior of involved devices as well as the utilized medium which is the radio waves naturally opened in a huge unpredictable and hostile atmosphere, wireless sensor networks are disclosed to various attacks more than any other networks:

Eavesdropping: this passive attack is the easiest attack against an opened network, in which an intruder with the enough hardware and software passively hear the transmitted data throughout the network for getting information about the network structure and the underlying routing protocols which can be utilized for future active attacks [19].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

***Data modification*:** This attack attempts to interrupt the transferred data forwarded from sensors to the BS and change the final report forwarded to the base station which can destroy the entire objectives of the deployed network, by forwarding false reports to the BS [19].

***Sink hole*:** also known as black hole attack, its purpose is to pull all the traffic from a specific region or node through a compromised node [20], by injecting fake routing information advertising the intruder as the legitimate sink or BS which forces the network traffic to pass over the intruder, for stopping the network facility or to execute other attacks i.e. data modification, man in the middle or eavesdropping etc.

***Selective forwarding*:** In selective forwarding attack, malicious nodes may deny to send particular messages and simply discard them, assuring that they are not propagated any more. In opposite of sink hole attack which can be easily determined, in selective forwarding the antagonist selectively sends packets and discard or changes other packets creating from a specified area or nodes and sends the remaining traffic which can make hard its detection [20].

IV. PUBLIC KEY CRYPTOGRAPHY FOR WSN

Public key cryptography also known as asymmetric cryptography utilizes two keys for encryption and decryption. In the manner that any message encrypted with one of the keys can only be decrypted with the other key. One of the keys is known as private key which is hold secretly by its holder, and the second one is publicly known by every entity in a provided community, utilizing these two keys, the public key cryptography can assure both integrity, confidentiality and authentication. Since, public key cryptography is neglected from the usage in WSNs, because of its high energy consumption and bandwidth which are very essential in sensor networks.

Table 1: Energy cost of digital signature (mJ)

Algorithm	**Sign**
RSA-1024	304
RSA-2048	2302,7
ECC-160	22,82
ECC-224	61,54

V. NETWORK ARCHITECTURE AND ASSUMPTIONS

In the rest paper we are going to show a security technique for wireless sensor networks based on public key cryptography as a tool for maintaining mutual authentication between base station and sensors.
Public key cryptography is utilized in our introduced technique to ensure the base station authentication however only the base station has a pair of asymmetric keys (private, public), the public key is preloaded for every sensor throughout the network before deployment, this key is utilized by sensors to authorize the BS and secure the handshake, which ensures the confidentiality and integrity of all dialogues with the base station, however only the BS has the valid private key for decryption. For managing effectively security throughout the network and to be utilized for all network configurations, we introduce to utilize two versions of our introduced technique the first one for flat networks and the second one for hierarchical networks. In flat network, sensor have the same roles and abilities, every sensor achieves environmental measure and forwards it to the base station utilizing the underlying routing protocol. Thus every sensor has responsibility for the connectivity with the BS. Finally, for our introduced technique, every sensor establishes a handshake with the BS for establishing a symmetric session key utilized for data encryption.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Sensors to Base Station Handshake
For securing data communication between base station and sensors, we introduce to establish a secure tunnel between them utilizing a symmetric shared key. This key is established utilizing a handshake encrypted with the public key of the BS to secure it from eventual attacks.

The sensor to BS handshake is executed in two steps:
Handshake launching: Every sensor over the network starts this operation by creating a random symmetric encrypting key. The created key is encrypted utilizing the public key of the BS and forwarded in a regular packet to the BS utilizing the specified routing protocol.
The usage of public key encryption for the handshake ensures:

- The authentication of the BS, however only the BS has the corresponding private key and can decrypts the message consisting the symmetric key.
- Integrity and confidentiality: no intermediary node can decrypt or read the message containing the symmetric key.

Session key Establishment: After the reception of the message consisting the session key, the BS decrypts this message utilizing the corresponding private key.
The base station records all the keys obtained from every sensor across the network in a global table, this table is utilized for identifying the sensors and their session keys. For validating the obtained session key, the base station forwards a challenge message for the corresponding sensor. If the corresponding sensor decrypts the challenge message forwarded by the BS, the handshake is successfully obtained and the two entities can utilize this key for future interaction, else a man in the middle attack is considered over this route which establishes a new handshake utilizing an alternative route.

VI. SECURING HIERARCHICAL NETWORK

Utilizing the specified clustering architecture in which the cluster head plays the primary part in the network management. We introduce to delegate the handshake operations and key update described above to cluster heads throughout the network which is going to decrease the overhead because of these two operations.
The handshake executed by every cluster head and the BS targeted to set up a symmetric shared key between the base station and sensors. This handshake is executed in three steps:

Symmetric key generation: Every cluster head creates a random symmetric key, encrypts this key with the public key of the BS and forwards it to the BS utilizing the underlying routing protocol in an ordinary packet. The usage of the public for transporting the session key assures handshake integrity, authentication and confidentiality.
Establishment of the session key: After obtaining and decrypting the message containing the session key coming from every cluster head, the BS records all the keys in a global table utilized for identifying and maintaining clusters across the network.

Completion of the handshake: For finishing and validating the handshake the BS creates a challenge message for every cluster head encrypted utilizing the established session key. Every cluster head decrypts this message if this operation success the handshake is successfully finished else the same operation is repeated until a valid session key is set up.
Distribution of the Session Key to Sensors: After a successful cluster head to BS handshake, every cluster member must get the same session key utilized by its cluster head. Thus, every cluster member makes a message consisting the cluster head identifier and a symmetric key utilized to protect the current operation, this message is encrypted utilizing the public key of the BS. When the base station obtains this message, it looks the availability of the corresponding session key of the cluster head (established during the prior handshake), encrypts it with the session key forwarded by the sensor and forwards it to that sensor. Every sensor when obtains this message from the BS, it shares the same session key with its cluster head and the BS which permit group security and data aggregation.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The dialogue is done with the BS rather than the cluster head because the BS is authorized utilizing its public key distributed before deployment.
System Functioning: Utilizing the same technique described for flat network to assure data integrity, we introduce to add a new field to the original packet structure which contains MAC (message authentication code) encrypted with the session key established in the prior handshake. The MAC can also be encrypted utilizing the public key of the BS if sensors have the essential resources to achieve this operation.
Key Update: After updating the cluster head session key, every cluster head encrypts a copy with the old session key for every cluster member. The new session key will be automatically utilized after obtaining the message by sensors in a provided cluster.

VII. METHODOLOGY & ALGORITHM

In our introduced technique, clustering is started by sensor nodes. Assume if any two key are process as Node A and Node B are two interacting sensor nodes in the WSN System. MCA is a cluster head within an ad hoc network, and it is chosen to offer distributed key management centre's service. KAB is the communication pair wise keys among nodes A and B. {M} PubA represents the message M encryption with Public Key of node A.

Step 1 A sensor node (Node A) flood a message, which consist its ID (IDA) to its neighbours.

Step 2 Every neighbour (Node B and others) should achieve the Public Key of Node A from MCA.

Step 3 Sensor Node B utilizes Sensor Node A's public key to encrypt messages which consist its identifier (IDB) and a random number (RN1), which is utilized to determine this transaction

Step 4 Sensor Node A forwards a message to Sensor Node B encrypted with PubB and consisting B's random no. (RN1) as well as a new random no. created by Node A (RN2).

Step 5 Sensor Node B chooses a secret key KAB and returns this and RN2, which are encrypted utilizing PubA, to ensure A that its correspondent is B.

Step 6 The interacting parties (Sensor Nodes) are agreeing on a Pair wise key and they can utilize this for protected communication.

Clustering is the procedure of scheduling objects into groups whose members are same in some manner, where one node in every cluster as cluster head, responsible for some tasks. Clustering offers a mutual organization of sensor nodes that eases transmission coordination between neighbouring nodes. This function decreases disturbance in multiple access broadcast atmosphere. Every cluster consist one or more sensor nodes and a cluster head (CH). The cluster head organizes the transmission of public key for every node in the cluster, this offers communicate rapidly among cluster members, which offers direct communication with a farther node. Additionally, a node moving in the same cluster without overlapping zone doesn't create any issue however it doesn't influence the cluster structure. The clustering method contains three kinds of nodes: Mobile Certification Authority (an administrator) which will be available only at the starting step then it can leave the network; a group of cluster head (CH) offers master services. Every node has a public and a private key. In the architecture, we assume that every cluster head is a mobile certification authority for its cluster members. To establish a protected WSN system, this decreases resource consumption and increases security performance. Consist of several nodes, which are distributed into a large region and one (or more) Mobile Certification Authority (MCA) and system coordination centre.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

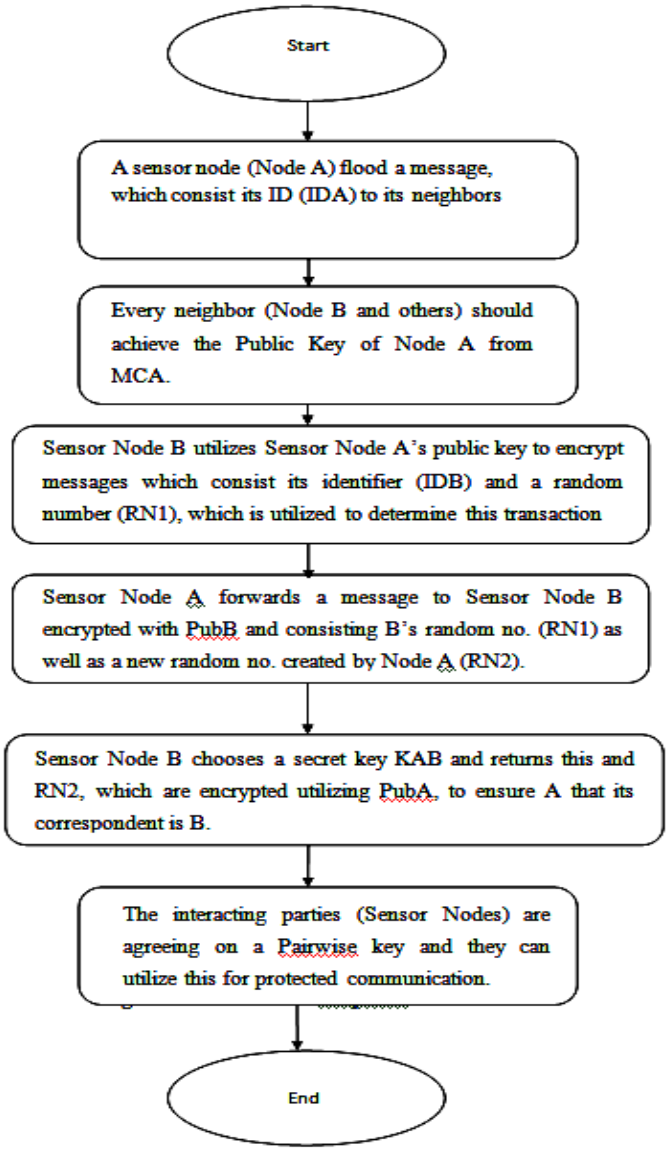

Fig. 2: Flow chart of proposed work

VIII. PERFORMANCE EVALUATION

The simulation results are examined and explained in various scenarios having networks of 100 sensor nodes for monitoring applications. In introduced framework, I have utilized symmetric key cryptographic Blowfish algorithm which is suitable to all three network level.

Comparison of Delay: It is concluded that during simulation for delay there is no fluctuation, and detect no delay when there has clustering mechanism used in comparison of second scenario. So according to the simulation the performance analysis of clustering mechanism is better in terms of delay.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

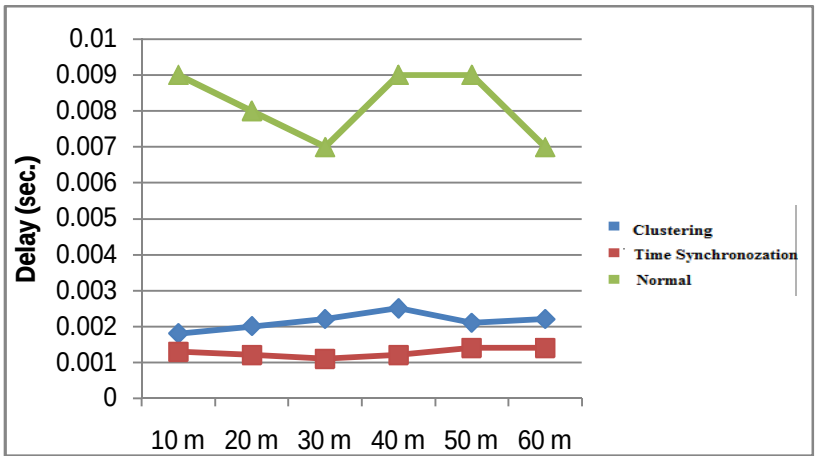

Fig. 3: Comparison of Delay

Comparison of Throughput: It is concluded that during simulation there is increase in throughput in comparison of other techniques when there has clustering technique is used.

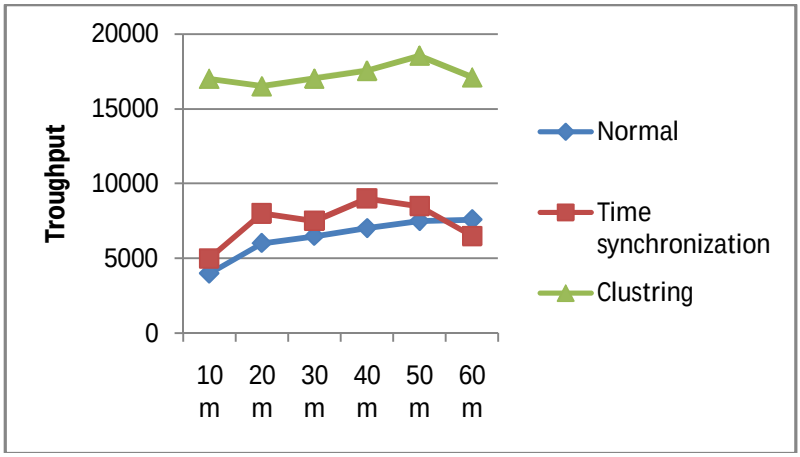

Fig. 4: Comparison of Throughput

IX. CONCLUSION

In this paper a protected symmetric key will be suggested for WSN. To secure against the attacks appropriate security techniques are needed Elliptic Curve Cryptography (ECC) is the best candidate because of its smaller key size. This thesis concentrates measure and improve the WSN routing protocol performance for monitoring of serious conditions with the help of important metrics i.e. throughput and delay with distinct mechanisms in many scenarios for mobile nodes and then enhance it by our suggested algorithm that depend on Encrypted Session keys.

The introduced key management is provided in two versions according to the network architecture hierarchical or flat. The first version is targeted to flat network and utilizes one handshake to share a symmetric encrypting key with the BS and every sensor throughout the network, the established session key is utilized to encrypt normal traffic.

The second version of the introduced technique treats the hierarchical architecture of WSNs in which the handshake operation and key update are assigned to cluster heads which play the primary role of the network security, this have considerably decreased the energy consumption in comparison of flat network version. From the security perspective it appears that the introduced key management ensures a great security threshold with a least energy consumption. In every scenario all nodes were utilized as source nodes of forward data to a common base station. So according to the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

simulation the performance analysis of clustering mechanism is better in terms of throughput and delay for mobile nodes.

REFERENCES

[1] Abedi, O.; Berangi, R.; Azgomi, M.A., "Improving Route Stability and Overhead on AODV Routing Protocol and Make it Usable forWireless Sensor Networks," in Proceedings of 29th IEEE International Conference onWireless Sensor Networks,June 2009, pp.464,467.
[2] Asha Rani Mishra, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network," International Journal of Engineering Research & Technology (IJERT) ,Vol. 1 Issue 3, pp. 2-3,May-2012.
[3] Bhoopathy, V. and R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2, pp.466-474,Mar-Apr 2012.
[4] Bharat Singh, Parvinder Singh & Dr. V.S. Dhaka, "Sensor Data Encryption Protocol for Wireless Network Security", Global Journal of Computer Science and Technology,Vol12,Issue 9, Version 1.0, April 2012.
[5] Chowdhury, S.I.; Won-Il Lee; Youn-Sang Choi; Guen-Young Kee; Jae-Young Pyun, "Performance evaluation of reactive routing protocols in Wireless Sensor Networks," in proceeding of Communications (APCC), 2011 17th Asia-Pacific Conference onad hoc networks ,*2011*, pp.559,564.
[6] C. Y. Wan, S. B. Eisenman, and A. T. Campbell,, "CODA: Congestion Detection and Avoidance in Sensor Networks," In Proceedings of FirstACM Conference on Embedded Networked Sensor Systems,2003,pp.266-279.
[7] Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", International conference on Information, Networking and Automation(ICINA),Kunming, IEEE, pp. 215-218, 2010.
[8] Fan Li and Yu Wang; " Survey of Routing in Wireless Sensor Networks",in Proceedings ofIEEE Wireless Sensor Networks Technology Magazine, Volume 2, Issue 2, June 2007; pp. 12-22.
[9]Gurjot singh, Ram singh , "A Secure Routing Scheme for Static Wireless Sensor Networks", IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol.2, pp.776-780, 2008.
[10] Harpreet Singh, Gurpreet Singh Josan, "Performance Analysis of AODV & DSR Routing Protocols in Wireless Sensor Networks", International Journal of Engineering ,Vol. 2, Issue 5,pp,2212-2216, September- October 2012.
[11] HeissenbüttelM., T. Braun, M. Wälchli, and T. Bernoulli, "Optimized stateless broadcasting in wireless multi-hop networks," in proceeding of 4th IEEE international conference on Infocom Barcelona,2006,pp.234-250.
[12]Hemanta Kumar Kalita and Avijit Kar "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009,pp.3-10.
[13] Jahanzeb Farooq, Bilal Rauf "Implementation and Evaluation of IEEE 802.11e WirelessLAN in GloMoSim" In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.
[14] Julio Lopez and Ricardo Dahab, "Fast Multiplication on Elliptic Curves over GF (2m)without Precomputation", Springer 2009
[15] KorkmazG., E. Ekici, F. Ozgüner, and U. Ozgüner, "Urban multi-hop broadcast protocolforWireless Sensor Networks," In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.