I.J. Information Technology and Computer Science, **2014, 08, 32-42**
Published Online July 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.08.05

Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes

Er. Gurjot Singh
Baba Banda Singh Bahadur Engineering College/ Computer Science & Engineering department, Fatehgarh Sahib, Punjab, India
Email: gurjotsingh52@yahoo.com

Er. Sandeep Kaur Dhanda
Baba Banda Singh Bahadur Engineering College/ Asstt. Prof., Computer Science & Engineering department, Fatehgarh Sahib, Punjab, India
Email: sandeep.tiwana@bbsbec.ac.in

***Abstract*—** A Wireless Sensor Network is a combination of spatially distributed independent nodes deployed in dense environment, communicating wirelessly over limited bandwidth and frequency. Security and Qos is the major concern in wireless sensor network due to its wireless communication nature and constraints like low computation capability, less memory, bounded energy resources, susceptibility to physical capture or damages and the use of insecure wireless communication channels. These constraints make security along with the QoS, a challenge in wireless sensor network. The cryptographic schemes increases the level of security and make it secure against critical attacks but also has a significant impact on the QoS of wireless sensor network. In this paper, the different cryptographic schemes based on asymmetric key and symmetric key cryptography are evaluated. The symmetric key cryptography schemes require less time for processing, less power and also require less storage space as compared to asymmetric key cryptographic schemes, results in less impact on the QoS of wireless sensor network. In this paper, the QoS of wireless sensor network along with cryptographic schemes will be evaluated on the basis of metrics like throughput, jitter, end-to-end delay, total packet received and energy consumption.

***Index Terms*—** QoS, Cryptography, ANODR, IPSec, ISAKMP, WSN`s.

I. Introduction

The Wireless sensor network is built of hundreds or even thousands of 'sensor nodes', where each node is connected to one or more sensors. Each such sensor nodes composed of several parts: a radio transceiver with an internal antenna or connection to an external antenna, a micro-controller and an electronic circuit for interfacing with the sensors and an energy source, usually a battery. The size and cost constraints on sensor nodes result in other constraints on resources like energy, memory, computational speed, Qos and communication bandwidth[1,2]. The Berkeley's MICA2 possess 4-8 MHz, 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency [3]. It is evident that there are limitations to what can be achieved through networking a number of these motes. Areas such as power management, network discovery, control and routing, information processing, quality of service and security are all currently under research [4].

Battery powered nodes are a common feature of many WSN applications. It is not feasible to replace or recharge the battery so are considered to be disposable. Many methods of powering these devices have been explored including solar power, but they remain to be seen typically as "one-use "devices [5]. Due to uncertain failures, their lifetime, QoS and productivity is extremely necessary to be maximized. Energy is the biggest constraint to wireless sensor capabilities. Once sensor nodes are deployed in a sensor network, it is not easy to replace or recharged it [6]. This notion of battery conservation extends to the primitives used to enforce security in WSNs. Security protocols strive to be light-weight, in terms of code size and processing requirements, while there is no degradation in their usefulness in achieving this goal [7].

The sensor networks require protection against eavesdropping and modification of propagated data packets. Cryptography is the standard method of defense against such attacks [4]. This defense brings with it a number of other trade-offs. Varying levels of cryptographic protection implies a proportionately varying level of overhead in the form of increased packet size, code size, processor usage and impact on the quality of service etc. However, the decision depends on the computation and communication capability of the sensor nodes. Since sensor nodes usually have severely constrained, asymmetric cryptography is often too expensive for many applications and also affect the quality of service of the network. Thus, effective approach is to use more efficient symmetric cryptographic alternatives [1,4]. These security schemes probably affect the quality of service of the network. It is extremely important to ensure that all known attacks are defended against when designing a security system for a WSN.

A. Quality of Service of Wireless Sensor Network

The quality of service is the ability of a network element such as a node to provide some level of assurance for a constraint data delivery. It is a group of service requirements to be met by the network while transporting a packet stream from source node to destination [8]. Due to the dynamic nature, limited resource availability and insecure transmission medium there is a need to maintain the quality of service for the wireless sensor network.

1. Quality of Service Challenges

Wireless sensor network inherit most of the well-known QoS challenges from traditional wireless networks such as security, unsecure transmission channel and unreliable links. However, typical characteristics of WSNs, such as severe resource constraints and harsh environmental conditions pose additional unique challenges for QoS-support [9, 10]. These QoS challenges for WSNs are explained in this section:

a. Security: Security is the major challenge in wireless sensor network. The wireless sensor network has limited resources like energy, memory and computation power etc. On increasing the security on wireless sensor network can affect the quality of service of the wireless sensor network. The cryptographic scheme that makes the WSNs secures against severe attacks could decreases its QoS too. The asymmetric key schemes are infeasible for wireless sensor network because these schemes require large storage space, long time for the processing of large algorithms and long size key for encryption/ decryption of data in WSN`s. On the other hand, the symmetric key based schemes require less time for processing, less storage space and small size keys for encryption and decryption of data makes them feasible for making secure wireless sensor network and also have less impact on quality of service of wireless sensor network.

***b. Mobility of sensor nodes*:** In wireless sensor network, sensor nodes are generally assumed to be static. However, some recent applications of WSNs, such as medical care and disaster response, utilize mobile sensor nodes and mobility poses another set of unique challenges to be addressed which include topology management, routing and energy management. Since the neighborhood of a node changes frequently due to the mobility, the topology and spatial density of the network also change frequently. Hence, QoS provisioning in mobile sensor networks become a more challenging task since envisioned methods must handle highly dynamic node connectivity and density. WSN related challenging issues are highlighted. These challenges make it difficult for providing deterministic QoS guarantees, such as packet delays, guaranteed bandwidth or packet losses in WSNs [9].

c. Resource constraints: WSNs lack of bandwidth, energy, memory and processing capability. However, limited energy is the most crucial one since in many cases it is impossible to replace or recharge batteries of the sensor nodes. Although energy harvesting via solar energy seems to be a promising solution to energy scarcity, present solar panels are still too large for tiny sensor devices. Eventually, proposed QoS support mechanisms must be lightweight and simple in order to operate on a highly resource constrained sensor node [9].

d. Node deployment: Deployment of the sensor nodes may be either uniform or random. In deterministic deployment, sensor nodes are placed by hand and routing can be performed through pre-scheduled paths. In a random deployment, sensor nodes are deployed randomly and organize themselves in an ad hoc manner. Hence, neighbor discovery, path discovery, geographical information of the nodes and clustering are the major issues to be solved [9].

e. Topology changes: Node mobility, link failures due to unsecure wireless communication, node malfunctioning, energy depletion or natural causes like flood or fire results in topology changes. Moreover, most of the link layer or MAC layer protocols employ sleep-listen schedules and turn the radio of the sensor nodes off temporarily for energy saving. This kind of power management mechanisms also cause frequent topology changes. Inevitably, dynamic nature of the WSN topology introduces an extra challenge for QoS support [9].

f. Scalability: Mostly the WSNs are composed of hundreds or thousands of sensor nodes. As the area of requirements for the quality of observation increase, more sensor nodes need to be deployed. Therefore, designed QoS mechanism must scale well with highly dense or large scale networks.

The aim of our research work is to implement the cryptographic schemes in wireless sensor network and to enhance their QoS with symmetric key cryptographic schemes. The remainder of this paper is organized as follow: the section 2, describes the different asymmetric and symmetric key cryptographic techniques. The section 3 covers the literature survey. The implementation of different cryptographic techniques and the impact of these on QoS of sensor network are presented in section 4 and 5. The last section concludes the paper.

II. Cryptographic Schemes for Wireless Sensor Network

Wireless sensor network are vulnerable to different types of attack that affect the performance i.e. QoS of wireless sensor network. To avoid this, different types of security schemes based of cryptography are applied to wireless sensor network to prevent it from these attacks. These schemes have significant impact on the QoS of the network.

A. Internet Protocol Security (IPSec)

IPSec is a collection of protocols designed by Internet Engineering Task Force (IETF) to provide security for a packet at network level. IPSec helps to create authenticated and confidential packets for IP layer.

Modes of IPSec Protocol

IPSec operates in one of two different modes i.e. transport Mode and tunnel mode.

a. Transport Mode: In this mode, IPSec protects the content that is delivered from the transport layer to the network layer. The transport mode protects the network layer payload by encapsulating it. Transport mode does not protect the IP header. In other words the transport mode does not protect the whole IP packet; it protects only the packet from the transport layer. The IPSec header and trailer are both added to information that is coming from transport layer after that IP header is added. The transport mode is normally used when we need host to host protection of data. The sender uses IPSec to authenticate and/or encrypt the pay load delivered from transport layer. The receiver uses IPSec to check the authentication and /or decrypt the IP packet and deliver it to the transport layer.

b. Tunnel mode: In this mode, IPSec protects whole IP packet. It takes an IP packet, including the header, applies IPSec security method to the entire packet, and then adds a new IP header. This new IP header has different information then the original IP header. The tunnel mode is used between a host and a router, between two routers, or between a router and a host. In other words, we use the tunnel mode when either the sender or the receiver is not a host. The entire original packet is protected from intrusion between sender and the receiver. It is as if the whole packet goes through an imaginary tunnel [11].

Security Protocols in IPSec

IPSec frameworks contains two protocols i.e. the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) Protocol to provide authentication and/or encryption for packet at the IP level.

a. Encapsulating Security Payload (ESP): It provides authentication, integrity and confidentiality, which protect the data from tampering and most efficiently, provide message content protection. IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms, that IPSec use to produce a unique and unforgeable identifier for every packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to ensure whether the data packets have been tampered or not. Furthermore, packets that are not authenticated are discarded and not delivered to the authorized receiver. It also provides all encryption services in IPSec. The encryption process translates the readable message (data) into an unreadable format that totally hides the message content that cannot be understood by any intruder. The decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the authorized sender/receiver to read the data. In addition to this, the ESP has another option to perform authentication, called ESP authentication. This ESP authentication provides authentication and integrity for the payload and not for the IP header [11]. In the present work, in ESP, the DES-CBC algorithm is used for encryption/decryption and HMAC-MD5 for the authentication. DES is a cipher block. It encrypts data in block, each of size 64 bits. In this the plain text of size 64 bits goes as the input to DES, which produces 64 bits of cipher text. The length of the key is 56 bits.

b. Authentication Header (AH): The authentication header protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet. The protocol uses a hash function and a symmetric key to create a message digest; the digest is inserted in the authentication header. The AH is then placed in appropriate location based on the mode. When an IP datagram carries an authentication header, the actual value in the protocol field of IP header is replaced by another value. The field inside the authentication header (the next header field) holds the original value of protocol field (the type of payload being carried by the IP datagram).

B. Internet Security Association and Key Management Protocol (ISAKMP)

Internet Security Association and Key Management Protocol (ISAKMP) is a basic framework of providing security in internet environment. ISAKMP provide support to other security protocols for creating and maintaining Security Associations in network. The ISAKMP host negotiates Security Association (ISAKMP SA) with other ISAKMP hosts and also with security protocols and services. ISAKMP Security Association is used to create user defined Security Association for negotiation between hosts [4]. The user defined Security Services, encryption algorithm, key exchange technique and authentication mechanism is created by coupling security Association with Authentication and key establishment mechanisms. In the present work, the security service in ISAKMP is followed by 3DES– CBC (Cipher Block Channing) and for authentication HMAC-SHA-1 is used and it operates on 64-byte blocks of data. Data Encryption Standard (DES) is landmark/ efficient cryptographic algorithm. DES is a block cipher. It encrypts data in blocks of size 64bits each which is given as input and it yields 64 bits of cipher text as output. It overcomes the problem of ECB (Electronic code block) that produce identical cipher text block as output for same input Cipher Block Chaining (CBC) algorithm yields totally different cipher text blocks in the output when identical plain text blocks are given as input to algorithm. The result of encryption of previous block is fed into encryption of current block [12].

C. Secure Neighbor Authentication

A protocol that deserves special attention from a security point of view is neighbor discovery (ND). One of the most basic requirements in a WSN is the ability of every node to reliably determine which of the other nodes are within its radio range so that it can establish single-hop communication links with them. Trustworthy neighbor discovery is an essential for securing higher-level network protocols and system abilities, such as physical and network access control, node localization and data routing [13]. In secure neighbor authentication each mobile node establishes an authenticated neighbor on the way path in the network. Each mobile node say (*a*)

broadcasts its identity packet< *SNAuth-HELLO, a*> to its neighborhood node in network.

In the pair-wise shared secret node (b), a neighboring receiver of the identity broadcast initiates a 3-way challenge-response handshake to authenticate node (a), the sender of the identity broadcast.

a. Suppose the nodes (a) and (b) share a pair-wise shared secret say k. Now the node (b) selects a random nonce say n1, encrypts this nonce n1 with k, sends the encrypted result *ENCk (n1*) to (a) by a message *<CHALLENGE, b, ENCk (n1)>*.

b. If the receiver of the challenge message send by the sender (b) is indeed node (a), then it can decrypt *ENCk (n1)* and sees n1. Then the node (a) selects another random nonce n2, encrypts *ENCk (n1 XOR n2),* and sends back *<RESPONSE1, a, n2, ENCk (n1 XOR n2)>* as the response to the challenger node (b).

c. When node (b) receives the response, then (b) decrypts *ENCk (n1 XOR n2)* and obtains n1 XOR n2. If the node (b) can get the same result from *XORing* n2 in the response and its own challenge n1, then node (a) passes the test with success. Otherwise, the node (b) does not send any packet to the node (a) and does not receive packets from node (a) except the response packets, until a correct <RESPONSE1> packet from node (a) can pass the test.

d. After detecting a success, the node (b) puts the node (a) in its secure neighbor list and the confirmation response is send back to the node (a) as follow:

Node (b) -> random nonce n3 and sends out a confirmation response *<RESPONSE2, b, n3, ENCk (n1 XOR n2 XOR n3)> to a.*

e. Upon receiving the RESPONSE2 message from node (b), the node (a) decrypts *ENCk (n1 XOR n2 XOR n3)* and retrieves *n1 XOR n2 XOR n3.* If this response message matches the result of XORing n1 that is previously decrypted its own n2 and n3 in the RESPONSE2 packet, then node (a) inserts node (b) into its secure neighbor list. In this way the challenge – response protocol ends [14].

The nodes insert themselves to each other neighbor node list and then they become authenticated to communicate with one another. The nonce length is set to 128-bit long [4]. Secure neighbor authentication is the essential need for other advanced network security services. In secure routing, the sender nodes forward packets for only those nodes that are detected by SNAuth. The Packets from other nodes not detected by SNAuth are dropped permanently.

D. Certificate Model

The certificate model implements for the purpose of authentication, authorization and access control. The digital signature systems are based on public key crypto systems, a signature signed by private key *SpK* can be verified by corresponding public key *PK,* and hence the signature cannot be verified or used by others who do not know the signing key *SpK*.

In a secured wireless network, each node must be capable of authenticating itself to its neighbor node (member) in a network. In this, every network member must acquire a signed credential from Certificate Authority (CA) prior to network operations. The credential is a signed by the CA's private key *SpKCA*, and can be verified by the well-known public key *PKCA*, which is assumed to be cached by every network member's local storage [4].

The certificate *CERTx* obtain by network member is in the form of *[X,pk*X*,validtime]* signed by *SpKCA* where unique id X is assigned to a node, pkX is the certified public key of the id X, and valid time limits the valid period of the certificate. If some nodes have multiple interfaces then that node must obtain different certificates for different interfaces in the network [15].

This certificate modeling is used for authentication services in the network. In this, the CA uses RSA algorithm for certificate generation. Public key algorithms such as RSA are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single-security operation [16]. It requires more storage space and consumes more power and time for its processing [17].

E. Anonymous On-demand Secure Routing protocol (ANODR)

ANODR is designed to provide an anonymous and untraceable routing scheme for wireless ad-hoc networks. It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless ad-hoc network [18]. The sensor networks have the requirement of sending the sensed data from multiple points to a common destination called sink. Resource management is required in sensor nodes regarding transmission power, storage, on-board energy and processing capacity. ANODR is based on table-driven AODV routing protocol. As in other routing protocols network routes are open to all i.e. packets sent in wireless manner then any adversaries can trace the network route and infer the pattern of the packets that are being communicate between communicating parties. This may pose a serious threat to network. The ANODR protocol allows you to protect the wireless communication from being traced and without removing your device`s battery. The adversaries should not trace the data packets that are sent by ANODR secure routing protocol. It provides untraceable path for data communication [17]. The threats of being eavesdropped by others are less. ANODR provides the following security services:

1. Negligibility- based anti-tracing such that signal interceptors cannot trace signal transmitters mobility pattern via wireless signal tracing (with non-negligible probability defined on the victim network's size).

2. Confidentiality and anonymity- The path follows by the packets should not be traced by any adversaries.

3. Identity-free routing- The identity cannot be stole by other.

One-time packet contents such that any two wireless transmissions are indistinguishable with each other in regard to a cryptanalyst. The ANODR configuration is based on AODV parameters. These services are provided at the Network and Link Layer to protect the IP and link layer protocols.

III. Literature Survey

Alwan and Agarwal [19] had presented a new routing mechanism, which integrates FEC codes and selective encryption scheme for providing both QoS and secure data transmission in WSN. In this proposed work, RS coding is used to provide reliability and security. The sink node decides on the paths selection process in order to satisfy the reliability or the delay requirements by an application and the number of these paths is determined to enhance the reliability.

Dadarlat [8] had examined the challenges of an adaptive monitoring framework (WSeH framework) with enhanced security and QoS support for WSNs, proposing a generic architecture and opening research issues.

Loong Yang et al. [20] had presented the scheme of key-agreement that is implemented on the modified Blom's scheme using multiple-keys which, while retaining the advantages of the basic scheme, improves it to make it very attractive for use in WSN. It achieve large pair wise key sizes, fast, and requires little energy and computational resources. They implemented the scheme in a MICAz mote and the results showed it be very advantageous compared other PKC schemes in terms of speed, energy, and RAM storage requirements. The network is fully secure if the number of compromised nodes does not exceed the capture threshold.

Zhang [21] had presented a Public Key Infrastructure for wireless sensor networks. The scheme tries to solve the problem of security in WSN by the use of public key cryptography as a tool for ensuring the authenticity of the base station. RSA is composed of two phases, the first is the sensor to base station handshake in which the base station and a given sensor node setup a session key to secure end to end link between them, this handshake is protected and authenticated using the public key of the base station. The second phase is the use of this session key for data encryption to ensure confidentiality and ensuring the integrity of the exchanged data using the MAC joined to each packet. It is energy efficient scheme.

Bhaskar et al. [22] had studied the QoS requirement in WSNs and highlighted some of the challenges posed by the unique characteristics of wireless sensor network. They have reviewed some of the QoS aware routing protocols for WSNs. A comparative study of some of the QoS aware routing protocols, taking few important parameters in context of WSNs is done. They have also discussed about the middleware based QoS support in WSNs. Finally, they had concluded by mentioning some of the open research problems in WSNs to initiate further research in the subject.

IV. Implementation Details

A. Implementation of cryptographic schemes

In the implementation of different Cryptographic schemes, the asymmetric key and symmetric key cryptographic schemes use different algorithms. These algorithms have their own specifications. The asymmetric key based cryptographic schemes such as secure neighbor model and certificate model use large key for encryption and decryption process. The certificate model scheme based on RSA algorithm uses key of size 1024 bits for certificate generation. For authentication, it use HMAC-SHA-1 algorithm. The symmetric key cryptographic schemes uses small size key for encryption and decryption process. The IPSe scheme is based on DES-CBC algorithms. It uses 56 bits of key size and 64 bits of block. For authentication and security, it uses HMAC-MD5 algorithm. The ISAKMP scheme is based on 3DES-CBC algorithm. It uses 112 bits key size. For security and authentication, it uses HMAC-SHA-1 algorithm. The table 1 and 2 shows the different cryptographic algorithms for encryption/decryption and authentication.

Table 1 symmetric key cryptographic algorithms

Algorithms	Key size (bits)	Block size (bits)	RFC Reference
DES-CBC	56	64	RFC-2405
3DES-CBC	112	64	RFC-2451

Table 2 MAC Algorithms

Algorithms	Key size (bits)	Output (bits)	RFC-Reference
HMAC-SHA1-96	160	96	RFC-2404
HMAC-MD5-96	128	96	RFC-2403

B. Simulation setup

QualNet 4.5.1 Network Simulator tool is used to evaluate the performance of different cryptographic schemes in wireless sensor networks. In the simulation scenario, the nodes are deployed randomly in a terrain of size of 1000*1000m. CBR is used as data traffic application with multiple source and destination. To configure the application and for mobility of nodes profile configuration, application configuration objects are included in scenario. It consists of basic network entities as sensor nodes (mobile) and PAN coordinator. The PAN coordinator used is fully functioned and other remaining nodes are reduced function devices having limited constraints like storage, energy and power. The security schemes like certificate model, secure neighbor model, IPsec, ISAKMP are implemented on sensor network. The affect of these schemes are analyzed i.e. the performance is measured on the basis of metrics like throughput, end-to-end delay, jitter, total packet received and energy consumption. The simulation time is 200 second. For simulation the different parameters are set are shown in table 3:

C. Simulation Scenario Design

In the scenario design of asymmetric and symmetric key cryptographic schemes in WSNs the nodes are placed randomly on terrain of size 1000* 1000m. The wireless cloud is placed on the terrain has configured to 802.15.4.

All the nodes are link wirelessly with the wireless subnet cloud. The nodes are made mobile nodes that move randomly on the terrain. CBR is used as data traffic application with multiple source and destination as shown in the fig. 1. Then different security schemes are configured on all the nodes and simulation is run for the scalability of nodes i.e. 10, 20, 30 and 40 nodes. The working of the simulation scenario of different cryptographic schemes is shown in fig. 2.

Table 3. Simulation parameters setup for QualNet simulator

Terrain Size	1000*1000
Simulation Time	200sec
Radio/Physical Layer	802.15.4
Mac protocol	802.15.4
No. of Nodes	10, 20, 30 and 40
Routing Protocol	AODV
Security Protocol	ANODR
Security Schemes	Secure Neighbor model, Certificate model, IPSec, ISAKMP
Traffic Type	CBR
Energy Model	Micaz
Mobility Model	Random Waypoint
Device type	PAN coordinator, FFD and RFD

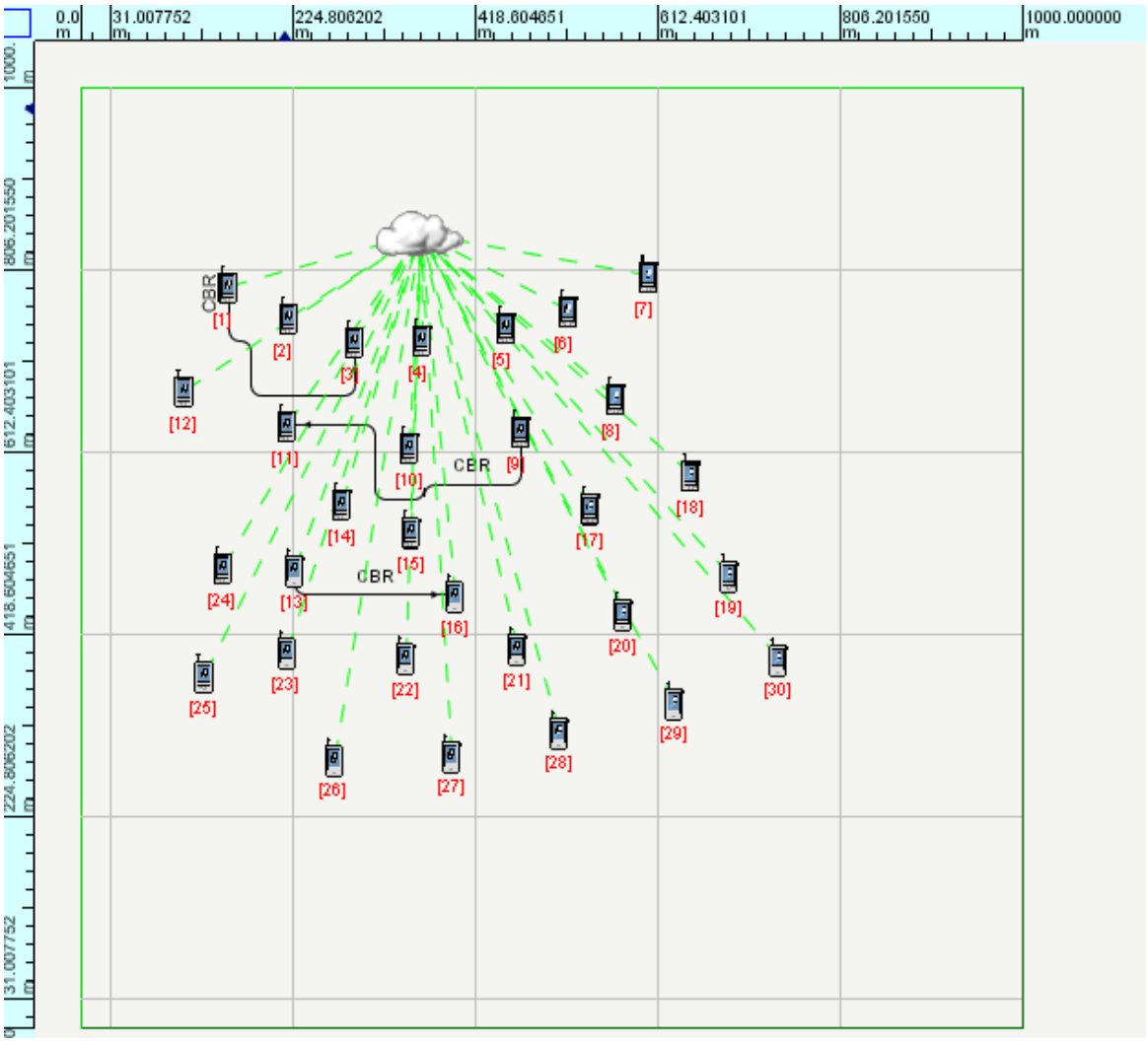

Fig. 1. Simulation scenario design

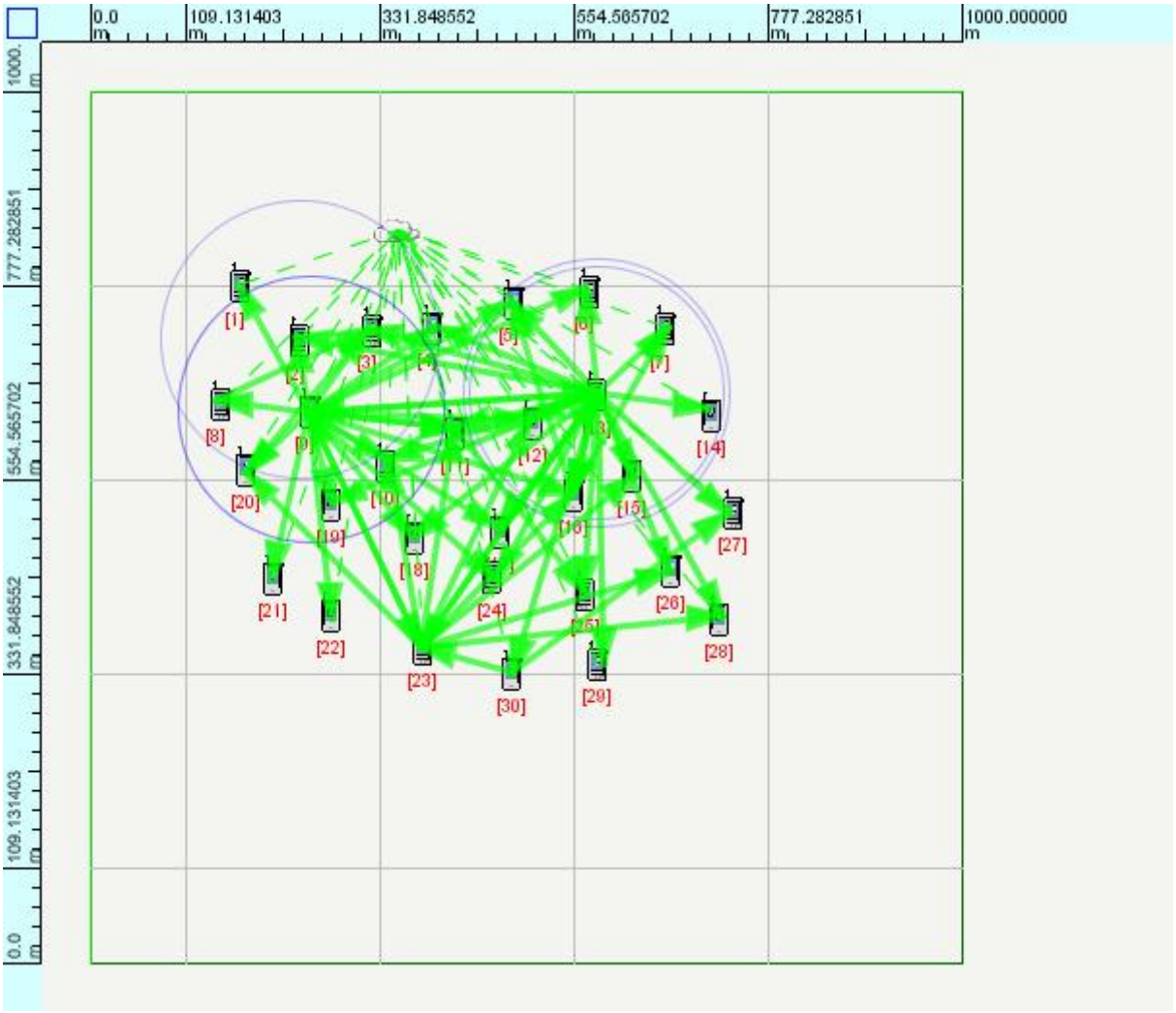

Fig. 2. Simulation working scenario

D. QoS parameters

In this section, we present the parameters that quantify the QoS. The general metrics from the networking perspective are maximizing throughput, minimizing end-to-end delay, maximizing reliability, maximizing energy efficiency, etc. The Security schemes can affect the QoS of the WSN. In order to perform well with security in mobile sensor nodes the choice of selecting efficient security schemes keeping in mind the limited constraints of wireless sensor network.

The throughput of the mobile wireless sensor network is maximized when numbers of packets received at the receiver node are nearly equal to the total number of packets send by the sender nodes. The asymmetric key cryptographic schemes have large size packets and also require more storage space so on changing topology of the WSN with mobility enable on sensor nodes the link between nodes are failed due to unreliable wireless transmission due to this, the packets are dropped and does not reach the destination results in the degradation in the throughput of the network [9, 10].

To minimize the end-to-end delay from sensor sources to the sink node, the performance of routing layer should also be taken into account. Theoretically, the asymmetric key cryptographic schemes require more storage space and time for their processing results in more end-to-end delay as compared to symmetric key based schemes. As the key sizes of asymmetric key cryptographic schemes are large to encrypt/decrypt the plain text to cipher text, the processing time is more. The jitter is the variation in the packets received by the receiver. The asymmetric key based schemes have high jitter value due to the more time consumed for the processing of the complex and long algorithms [9].

Energy efficiency is still the most important requirement in WSNs due to the battery-limited operation of sensor devices. MAC layer can contribute to energy efficiency by minimizing collisions and retransmissions. The asymmetric key schemes require more energy because of large size of the data packets as compared to symmetric key based cryptographic schemes. Wireless operation consumes most of the energy and radio should be kept off whenever it is not needed. WSNs are characterized by their dynamic behavior. Nodes may deplete their battery and disconnect from the network, new nodes may be added to the network, links between nodes may change in time due to environmental conditions or topological changes, traffic conditions may change according to the monitored phenomena[9].

V. Result and Discussion

This section evaluates the performance of different asymmetric and symmetric key cryptographic schemes in wireless sensor network. After describing our implementation and simulation setup, we evaluate the impact of different security schemes like IPsec, ISAKMP, Secure neighbor model, certificate model and ANODR on the quality of service parameter like throughput, end to end delay, jitter, packet received and energy consumption of wireless sensor network. The cryptographic security schemes had impact on the quality of service of the wireless sensor network due to its limited constraints.

A. Throughput (bits/s) -

The fig. 3 shows the throughput of different cryptographic schemes in WSN`s. The throughput of IPsec security scheme is more than other security schemes and there is slight degradation in the throughput when the number of nodes increases. It is based on symmetric key cryptographic scheme and operates on DSE-CBC with HMAC-SHA algorithm for encryption/decryption and authentication. The throughput of the certificate model decreases rapidly as the number of nodes increases. It is based on asymmetric cryptography scheme using RSA with HMAC-SHA algorithm for certificate generation and authentication. The throughput of symmetric key cryptography scheme name, IPsec is 928.1 bits per sec. more than that of asymmetric key scheme named certificate model as shown in fig. 3. The symmetric key cryptographic schemes performs best for wireless sensor network as there is less degradation in throughput than asymmetric cryptographic schemes.

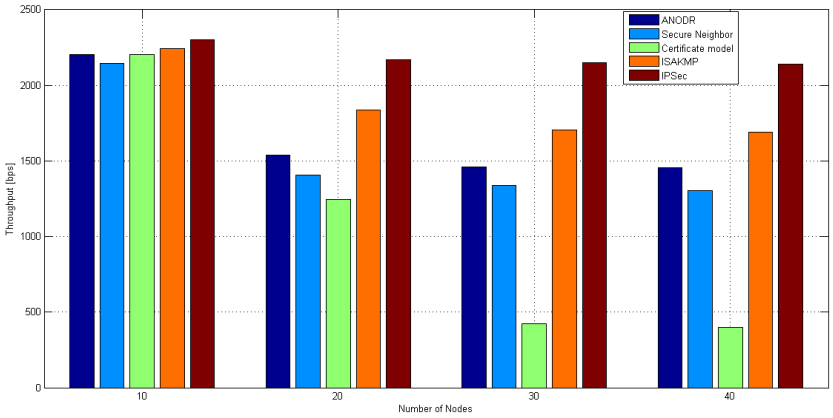

Fig. 3. Throughput

B. End-to-end delay (sec.) -

The asymmetric cryptographic schemes have more end-to-end delay than symmetric key cryptographic schemes. The public key cryptography schemes acquire more storage space because of large size. It also require more time for processing of long algorithm than private key cryptography schemes. In this, the end-to-end delay of certificate model is very high and it increases rapidly as the number of nodes increases as shown in fig. 4. It uses RSA public key algorithm for certificate creation. The symmetric key cryptographic schemes have less end-to-end delay. The end-to-end delay of symmetric key cryptography scheme name ISAKMP is 0.62796 seconds less than asymmetric key based cryptographic schemes as shown in fig. 4. The IPsec security scheme also has less end-to-end delay. With increase in number of nodes the end-to-end delay for all security schemes increases but in ISAKMP schemes it increases slowly.

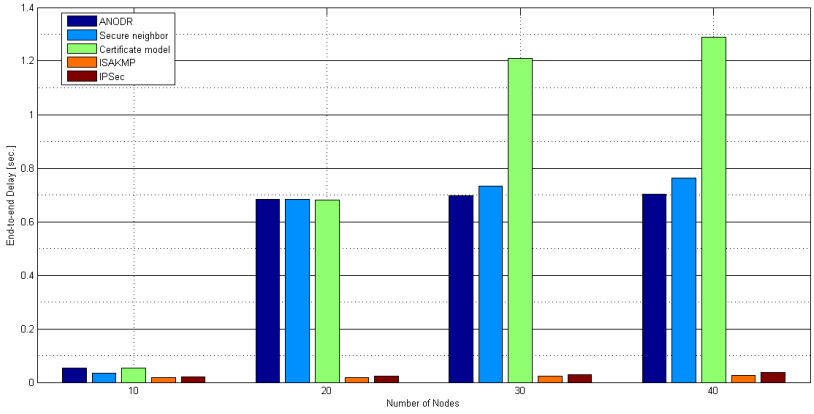

Fig. 4. End-to-end delay

C. Energy consumed in transmit mode (mj)-

The above fig. 5 shows that the secure neighbor model consumes more energy and it increases rapidly when number of nodes increases, so it's considered as worst in case of energy transmit mode. The energy consumption of IPsec security scheme is very less as compared to other security schemes and it decreases as the number of nodes increases so it is considered as best security schemes for wireless sensor network. The symmetric key scheme consumes 0.0160516mj less amount of energy in transmit mode than asymmetric key based schemes as shown in fig. 5. The ISAKMP security schemes also consumed less amount of energy as number of nodes increases than other asymmetric key cryptographic based schemes.

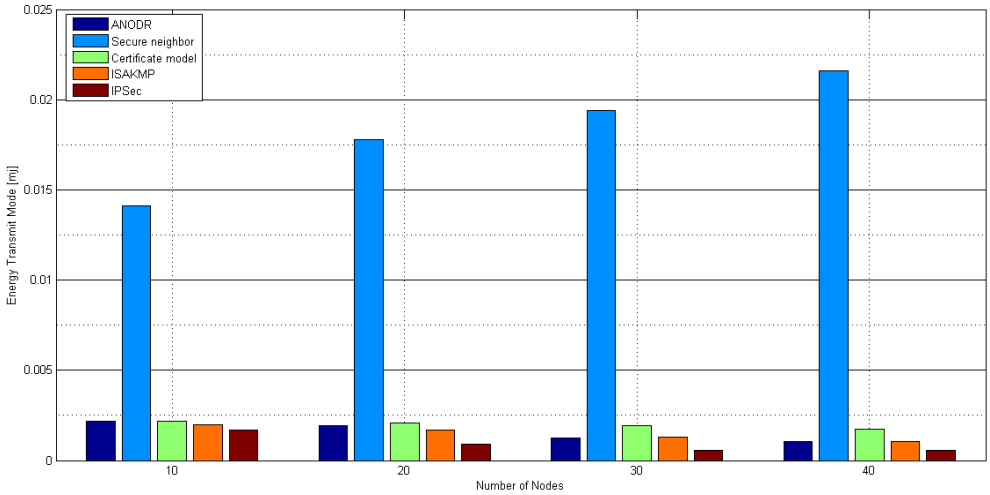

Fig. 5. Energy Consumed in Transmit mode

D. Energy consumed in receive mode (mj)-

The fig. 6 shows that the secure neighbor model scheme consumes more energy in receive mode as compared to other cryptographic schemes and its energy consumption increase rapidly as the number of nodes increases. The IPsec security scheme again consumed less amount of energy as compared to other security schemes. The symmetric key cryptographic scheme consumes 0.037991mj less amount of energy than asymmetric key based cryptographic schemes as shown in fig. 6.

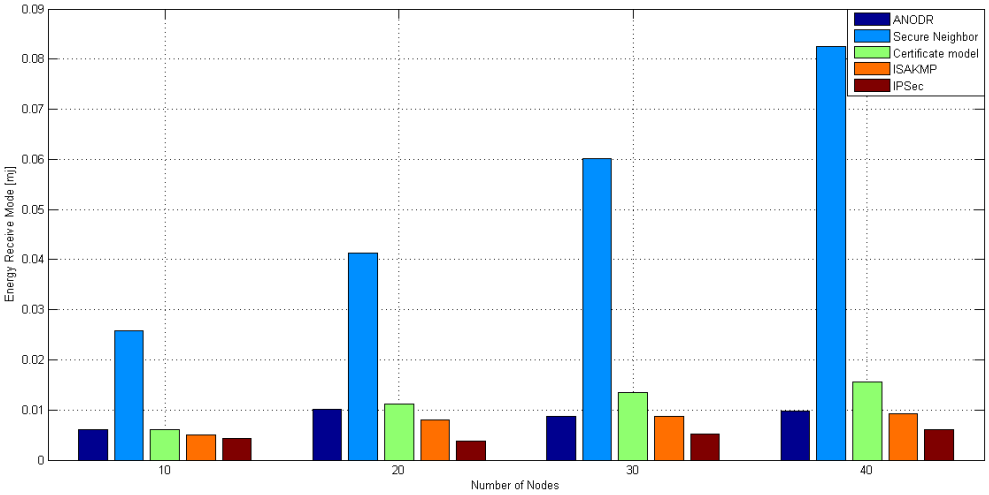

Fig. 6. Energy Consumed in Receive mode

E. Total packet received-

The total packets that are sent in the one set of simulation for different cryptographic schemes are 48. In symmetric key based schemes the total number of packet received are more as compared to asymmetric key based schemes. The packet loss is more in asymmetric key based schemes than in symmetric key based. The total packet received by IPSec i.e. symmetric key based schemes is 177 out of 192 packets (192 packets is sum of scalability of nodes i.e. 10, 20, 30 and 40 nodes) and in ANODR i.e. asymmetric key based schemes is 117 out of 192 packets as shown in fig. 7.

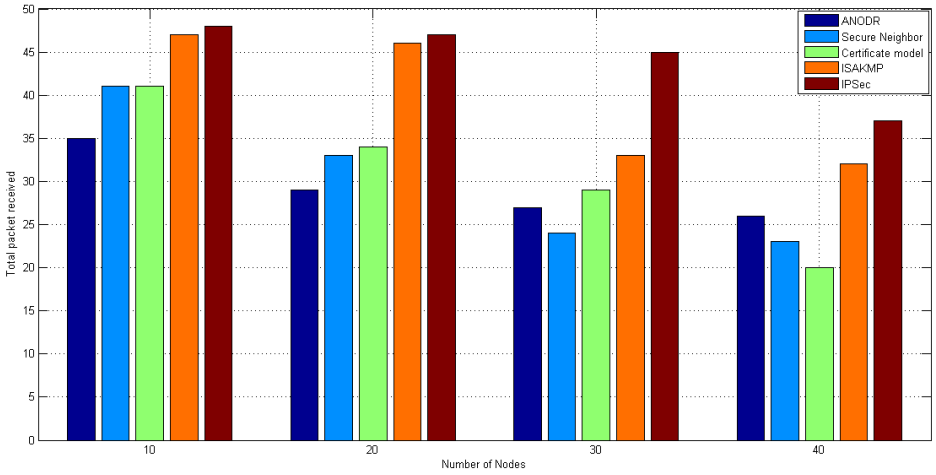

Fig. 7. Total packet received

5.6. Jitter (sec.) –

The network is considered to be efficient and reliable if its jitter as well as the packet drop ratio is less. The symmetric key based schemes have less jitter than asymmetric key based schemes. The IPSec and ISAKMP i.e. symmetric key based schemes have less jitter and it increases as the number of nodes increases but very less as compared to asymmetric key based schemes i.e. ANODR, secure neighbor model, certificate model as shown in fig. 8. The certificate model scheme has more jitter than other schemes.

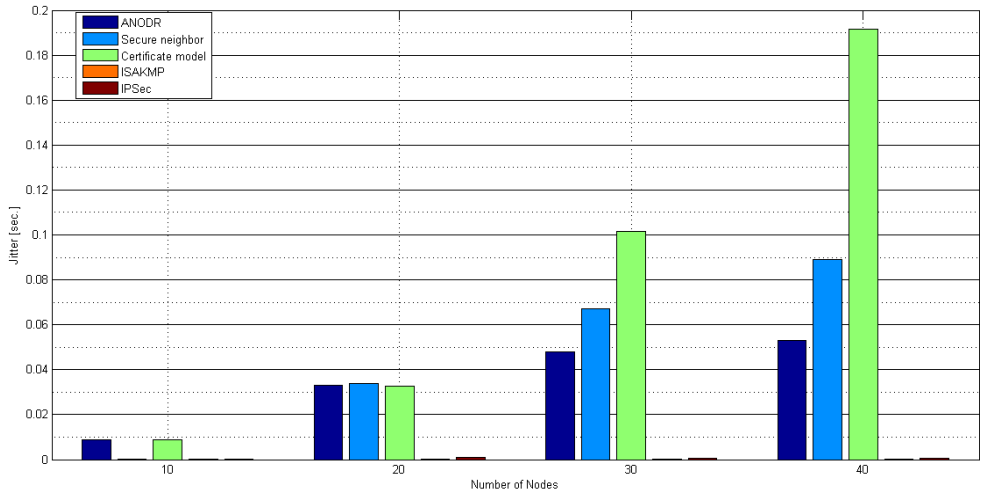

Fig. 8. Jitter

VI. Conclusion

In this paper, different cryptographic schemes based on symmetric and asymmetric keys are presented and how they affect the QOS of wireless sensor network is investigated on the basis of metrics like throughput, end-to-end delay, jitter, total packet received and energy consumption. The performance is generally degraded with the addition of security services in WSNs. As is evident, Symmetric key cryptography based schemes have been the main source of security in Wireless Sensor Network, to date. The selection of the effective cryptographic schemes depends on the processing capability of the sensor nodes characterized by the constraints on energy, computation capability, less memory and communication bandwidth. The mobility of sensor nodes has a great influence on sensor network topology. Mobility can be at the base station and also on sensor nodes may affect the QOS of wireless sensor network. The asymmetric key cryptographic schemes affect the QOS of wireless sensor network more than symmetric key cryptographic schemes. It is concluded from the simulation that the throughput of symmetric key schemes is more as compared to asymmetric key cryptographic schemes. The throughput of IPSec symmetric key cryptographic scheme is more than other cryptographic schemes as shown in fig 3. It operates on DES-CBC algorithm. From an authentication perspective, the CBC-MAC algorithm is the most popular method of providing authentication for symmetric key based algorithms.

The end-to-end delay of asymmetric key cryptographic schemes is more than symmetric key based cryptographic schemes. The certificate model scheme has more end-to-end delay than all other schemes and it increases rapidly

with scalability of nodes. The symmetric key cryptographic scheme name ISAKMP has very less end-to-end delay among all cryptographic schemes as shown in fig 4. The asymmetric key cryptographic schemes require more storage space and time for their processing.

The jitter and the packet loss of asymmetric key based schemes are more than symmetric key based schemes. The symmetric key based scheme named IPSec has less jitter and less packet loss rate than other cryptographic schemes as shown in fig. 7 and 8.

The energy consumption of symmetric key based schemes is less as compared to asymmetric key cryptographic schemes. The symmetric key based cryptographic scheme named IPSec consumed less amount of energy both in energy transmit and receive mode as shown in fig 5 and 6.

The QOS of symmetric key based cryptographic schemes are better than asymmetric key based schemes for wireless sensor network. The IPSec symmetric key based cryptography scheme has high QOS than other cryptographic schemes.

REFERENCES

[1] Granjal Jorge, Monteiro Edmundo and Silva Jorge Sa,"A secure interconnection model for IPv6 enabled Wireless Sensor Networks", IEEE, pp. 1-6, 2010.

[2] Johnson M., Healy M., Van de Ven P., Hayes M., Nelson J., Newe T. and Lewis E., "A Comparative Review of Wireless Sensor Network Mote Technologies", IEEE Sensors, 2009.

[3] Chaudhari H.C. and Kadam L.U., "Wireless Sensor Networks: Security, Attacks and Challenges", International Journal of Networking, Vol. 1, No. 1, pp. 4-16, 2011.

[4] Gurjot Singh and Sandeep Kaur Dhanda, "Performance Analysis of Security Schemes in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue. 8, pp. 3217- 3223, 2013.

[5] Granjal Jorge, Monteiro Edmundo and Silva Jorge Sa, "Enabling network-layer security on Ipv6 Wireless Sensor Networks", IEEE Globecom pp. 12- 18, 2010.

[6] Dr. Jain Kumar Manoj, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT, Vol. 2, No. 1, pp. 62-67, 2011.

[7] Shahriar Mohammadi, Reza Ebrahimi Atani, Hossein Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security, vol. 2, pp. 69- 84, 2011.

[8] Dadarlat Vasile, "WSeH: Proposal for an Adaptive Monitoring Framework for WSNs, with Enhanced Security and QoS Support", IEEE, pp. 7-12, 2012.

[9] M. Yigitel Aykut, Incel Ozlem Durmaz, Ersoy Cem, "QoS-aware MAC protocols for wireless sensor networks: A survey", Elsevier- Computer Networks, 55, pp. 1982-2004, 2011.

[10] P. Rajan and S. Varatha Rajan, "Network Supporting Multilayered Quality of Service Routing in Wireless Sensor Networks" PROCEEDINGS OF ICETECT- IEEE, PP. no. 1016- 1025, 2011.

[11] Raza Shahid, Chung Tony, Duquennoy Simon, Yazar Dogan, Voigt Thiemo and Roedig Utz, "Securing Internet of Things with Lightweight IPsec", SICS, Vol. 8, pp. 1-26, 2011.

[12] Dr. Padmavathi G., Dr. Subashini P. and Devi Aruna D., "DSSS with ISAKMP Key Management Protocol to Secure Physical Layer for Mobile Adhoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol. 4 No. 1, pp 69-76, 2012.

[13] Garcıa-Otero Mariano and Poblacion-Hernandez Adrian, "Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques", International Journal of Distributed Sensor Networks, Vol. 5, pp. 1-12, 2012.

[14] Devi Aurna D. and Subashini P., "SNAuth-SPMAODV: Secure Neighbor Authentication Strict Priority Multipath AODV against Denial of Service attack for MANET in Military Scenario", International Journal of Computer Applications, Vol. 48, No. 4, pp. 1-6, 2012.

[15] Ramannavar Manjila M. and Jagtap Monica M., "Authentication in Wireless Sensor Networks Using Virtual Certificate Authorities", International Journal of Emerging Technology and Advanced Engineering , Volume 2, No. 11, pp. 81-85, 2012.

[16] Sen Jaidip, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, pp. 55- 78, 2009.

[17] Kahate Atul, "Cryptography and network security", The Tata Mcgraw- hill, 2003.

[18] Kong Jiejun and Hong Xiaoyan, "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks", ACM, 2004.

[19] Alwan Hind and Agarwal Anjali, "A Secure mechanism for QOS routing in wireless sensor networks", IEEE, 2012.

[20] Yang Loong Mee, Al-Anbuky Adnan and William Liu, "A Fast and Efficient Key Agreement Scheme for Wireless Sensor Networks", International Conference on Wireless and Mobile Communications, Vol. 5, pp. 231-237, 2012.

[21] Yu Zhang, "The Scheme of Public Key Infrastructure for Improving Wireless Sensor Networks Security", IEEE, pp. 626-629, 2012.

[22] Bhuyan Bhaskar, Deva Sarma Kumar Hiren, Sarma Nityananda, Avijit Kaur Avijit and Mall Rajib, "Quality of Service (QoS) Provisions in Wireless Sensor Networks and Related Challenges", Wireless Sensor Network- Scientific research, no. 2, pp. 861- 868, 2010.

Authors' Profile

Er. Gurjot Singh: He received his B.Tech. degree in computer science and engineering from Guru Nanak Dev Engineering College, India and his Master`s degree in computer science and engineering (specialization E-Security) from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India. His research area includes security in wireless network (Adhoc, Sensor network).

Er. Sandeep Kaur Dhanda: She received her Master`s degree in computer science and engineering from Thapar University, Patiala, Punjab, India. Presently, she`s a assistant professor at computer science and engineering department of Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, India. Her research area includes parallel computing.