ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

Performance Analysis of Security Schemes in Wireless Sensor Network

Gurjot Singh[1], Er. Sandeep Kaur Dhanda[2]

Student, CSE/IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab), India[1]
Asst. Prof., CSE/IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab), India [2]

Abstract: A Wireless Sensor Network (WSN) is a group of independent nodes, communicating wirelessly over limited frequency and bandwidth. The novelty of WSNs in comparison to traditional sensor networks is that they depend on dense deployment and coordination to execute their tasks successfully. Wireless Sensor Networks are used in many applications like military, ecological, and health-related areas. Security is the major concern in WSN due to its wireless communication nature and constraints like low computation capability, small memory, Bounded energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security a challenge to WSNs. The cryptographic schemes increases the security level and make it secure against different attacks. In this paper, different asymmetric and symmetric key cryptographic based security schemes like secure neighbour model, certificate model, ISAKMP (internet security association and key management protocol), IPSec (Internet protocol Security) and secure routing (ANODR i.e. anonymous on demand routing) are compared on WSNs. Providing security to sensor networks has a significant impact on QOS of sensor network. In this paper the QOS of WSN along with security schemes will be evaluated on the basis of metrics like throughput, end-to-end delay and energy consumption.

Keywords: WSN- wireless sensor network, ISAKMP- Internet security association and key management protocol, IPSec- Internet protocol security, ANODR- Anonymous on-demand routing, CA- Certificate authority

I. INTRODUCTION TO WIRELESS SENSOR NETWORK

A wireless sensor network (WSN) consists of spatially distributed autonomous mobile nodes and sensors to monitor physical or environmental conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location. The development of wireless networks was motivated by military applications such as battlefield surveillance. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. Consider the Crossbow "MICAz" mote, currently a typical mote used in WSNs. It consists of a battery, 4Mhz-8Mhz microcontroller, microprocessor (Atmega128), RF transceiver, ADC, 128K bytes Program Flash Memory and 4K bytes EEPROM, 48-256kB of instruction memory [14]. Berkeley's MICA2 possess 4-8 MHz, 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency [1]. 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, collaborative signal and information processing, tasking and querying, and security are all currently under research [3]. Battery powered nodes are a common feature of many WSN applications, where recharging or replacement would not normally be feasible, and 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 [2]. Eventual failure is expected and so maximizing their lifetime and productivity is extremely important. Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced or recharged [13]. Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. 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, whilst retaining their usefulness, in order to assist in achieving this goal. To design a completely secure WSN, security must be integrated into every node of the system. Any component of a network implemented without any security could easily become a point of attack. Resultantly, this dictates that security must pervade every aspect of the design of a wireless sensor network application that would collect or disseminate sensitive information; i.e. requiring a high level of security [3].

Conventional networks require protection against eavesdropping, injection or modification of disseminated data packets, and accordingly, most applications of WSNs require the same protection. Cryptography is the standard

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

method of defence against such attacks [3]. This defence brings with it a number of other trade-offs. 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. Thus, a promising approach is to use more efficient symmetric cryptographic alternatives [9]. This is the stem of all debate relating to optimal security techniques in WSNs. It is extremely important to ensure that all known attacks are defended against when designing a security system for a WSN. The success of the application will depend largely upon its reliability and robustness against attack. There are many obstacles and constraints involved when designing a security protocol for WSNs. The limited memory, storage and processor capabilities, coupled with stringent power limitations distinguish WSN security architecture design requirements from any other. Harsh environmental operating conditions, the threat of physical compromise and unreliable data transfer also provide challenges for designers. Intended application areas are intrinsic to what type/level of security is required. Limited only by what can be technologically sensed, the door is open for applications of WSNs in all walks of life.

II. SECURITY SCHEMES FOR WIRELESS SENSOR NETWORK

WSN are vulnerable to different types of attack that affect the performance of network. To avoid this different types of security schemes based of cryptography are applied on wsn to secure them from these attacks.

A. Secure Neighbour Authentication- A protocol that deserves special attention from a security point of view is neighbour discovery (ND). This is because 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 links with them. Trustworthy ND is a cornerstone for securing higher-level network protocols and system functionalities, such as physical and network access control, data routing, and node localization [4]. In this mechanism each node establishes an authenticated neighbour on the way path in the network. Each mobile node broadcasts its identity packet to its neighbourhood node in network.

In the pair-wise shared secret mode, a neighbouring receiver of the identity broadcast initiates a 3-way challenge-response handshake to authenticate sender [5]. The authentication process is as follows.

A. Firstly two communicating nodes say X and Y share a secret key. Y sends an encrypted packet to other node through challenge message.

B. If the receiver of the challenge message is intended receiver X, and then it can decrypt the packet and read the message. Then X selects another random packet, encrypts it by using XOR operation and sends back as response to challenger Y.

C. On receiving response, Y decrypts it and obtains the original packet. If Y can get same result from XORing that encrypted packet then X passes the test with success otherwise Y doesn't send any packet to X.

D. After the success Y puts X in its secure neighbour list and then confirmation response is send back to X

E. upon receiving this response 2 from Y, the node X decrypts it and matches the result. In this way the challenge –response protocol ends. In this way all the nodes insert themselves to each other neighbour node list and then they become authenticated to communicate with each another. The packet (nonce) length is currently set to 128-bit long.

B. 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 can be verified by corresponding public key and hence the signature cannot be verified or used by others who do not know the signing key.

In a secured wireless network, each node must be capable of authenticating itself to its neighbour node (member) in a network. The Certificate Authority (CA) will assign a signed credential to every node (member) in a network. The credential is a certificate signed by the Certifying Authority's private key and can be verified by the well-known public key which is assumed to be cached by every network member's local storage. A unique id is assigned to every node in a certification process. If some nodes have multiple interfaces then that node must obtain different certificates for different interfaces in the network. This certificate modelling is used for authentication services in the network. In this, the CA uses RSA algorithm for certificate generation. The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm. 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 [10]. In this the prime number are the basis of the RSA algorithm. A prime number is the one that is divisible only by 1 and itself. For instance, 3 is a prime number because it can be divided only by 1 or 3. However, 4 is not a prime number, because other than by 1 and 4, it can be divided by 2.

The RSA algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large prime numbers.

It requires more storage space and consumes more power and time for its processing [7].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

C. Internet Security Association and Key Management Protocol - 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 (SAs) in network. The ISAKMP host negotiates Security Association (ISAKMP SA) with other ISAKMP hosts and also with security protocols and services [6]. ISAKMP Security Association is used to create user defined Security Association for negotiation between hosts. User defined Security Service, key exchange technique, encryption algorithm, and authentication mechanism is created by coupling security Association with Authentication and key establishment mechanisms. Security Service in ISAKMP is followed by 3 DES- CBC (Cipher Block Channing) and for authentication HMAC-SHA is used and it operates on 64-byte blocks of data. Data Encryption Standard (DES) is landmark in 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.

D. Internet Protocol Security (IPsec) - IPSec is a standard suite of protocols prescribed by Internet Engineering Task Force (IETF), which provides data authentication, integrity, and confidentiality to data between communicating points across IP networks. IPSec provides data security at the IP packet level. It provides end-to end security. It operates at internet layer of the internet protocol suite. IPSec works in two modes that are tunnel mode and transport mode. Transport Mode protects packets coming from transport layer to network layer by encapsulating the payload only but doesn't encapsulate the header. The IPSec header and trailer are added to message coming from transport layer. Transport mode is used when Host-to-Host protection of data is required. In tunnel mode whole packet is protected along with the header. The IP header is added in this mode. Tunnel mode is used when communication occurs between two routers, between a host and a router, or a router and host. There are two protocols in IPSec suite: Authentication header (AH) protocol and Encapsulating Security Payload (ESP) that provides authentication and encryption for packet security. Authentication header protocol authenticates the source host and ensures the payload integrity carried in IP packet. This protocol uses hash function and symmetric key to create the message digest; digest is inserted into authentication header and then AH is placed in appropriate place according to the mode. AH protects against unauthorized retransmission of packets by providing optional anti-replay protection. Authentication Header provides authentication and integrity, but doesn't provide privacy or confidentiality. If data is intercepted and only AH is used, the message contents can be read. For providing privacy or confidentiality Encapsulating Security payload (ESP) is used, which protect AH protects against unauthorized retransmission of packets by providing optional anti-replay protection against data tampering and most importantly provide message content protection. IPSec provides an open framework for implementing standard algorithms, such as MD5. These algorithms generate unique and unforgeable identifier for each packet, which is a data equivalent to a fingerprint. If some packets are tempered by intruder than this unique identifier helps in determining the tampered data. Along with Encryption/Decryption the ESP has an option to perform authentication that is called ESP authentication, using ESP authentication ESP provides authentication and integrity for the payload and not for the IP header. The authentication algorithms are compared separately for AH and ESP: with AH the MAC is calculated over the IP header and payload packet, while in ESP the IP header is neither encrypted nor authenticated [11]. The computational and energetic demands introduced by cryptography, although significant, do not compromise the applicability of security solutions such as IPSec on sensor nodes. The new sensor nodes have more storage space than traditional devices i.e. sensor devices [12].

III. SECURE ROUTING PROTOCOL

Wireless networks are different from other contemporary communication and wireless ad hoc networks routing is a very challenging task in WSNs. For the deployed sheer number of sensor nodes it is impractical to build a global scheme for them. All applications of 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. For Security purposes, a secure routing protocol (ANODR) is used for routing in WSN. It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless ad-hoc network.

A. Anonymous on-demand Routing (ANODR) Protocol - It is designed to provide an anonymous and untraceable routing scheme for wireless ad-hoc networks. It 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. It's a challenging constraint

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

for routing and data forwarding. 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. The threats of being eavesdropped by others are less [8]. 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 follow by the packets should not be traced by any adversaries..

3. Traffic flow confidentiality- Conceals the message content through encryption.

4. Identity-free routing- The identity can not be stole by other.

5. 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 parameter settings. ANODR parameters use the same terminology as AODV's parameters, except the name is changed from AODV to ANODR. These services are provided at the Network Layer and Link Layer to protect the IP and link layer protocols.

IV. IMPLEMENTATION

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 secure neighbour model and certificate model is based on asymmetric key cryptography. The ISAKMP and IPSec is based on symmetric key cryptography. The asymmetric key cryptographic schemes use RSA with SHA for encryption/decryption and symmetric key schemes uses DES-CBC, MD5 and 3DES-CBC, SHA algorithms for encryption/decryption and authentication procedures.

A. SIMULATION ENVIRONMENT

QualNet 4.5.1 Network Simulator tool is used to evaluate the performance of different security schemes in wireless sensor networks. In the implementation, the nodes are deployed randomly in a terrain of size 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 and application configuration objects are included in the 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 energy, power etc. The security schemes like certificate model, secure neighbour model, IPSec., ISAKMP are implemented on sensor network. The affect of these schemes are analysed i.e. the performance is measured on the basis of parameters like throughput, delay and energy consumption. The simulation time is 200 seconds. For simulation the values of different parameters used are as follows:

B. Simulation parameters

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

C. Simulation Scenario

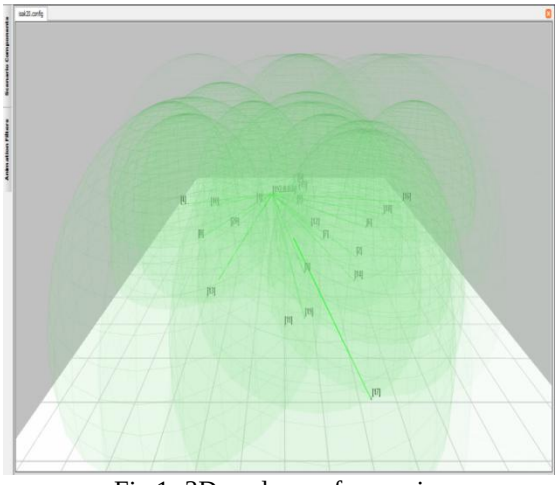

Fig.1- 3D analyser of scenario

V. RESULT AND EVALUATION

We evaluate the performance of different cryptographic schemes on the basis of metrics like throughput, end-to-end delay and energy consumption. The cryptographic security schemes had impact on the quality of service of the wsn because of limited constraints. To analyze the performance of the security schemes by varying the nodes, the metrics used to evaluate the performance are given below.

A. Throughput: Throughput of different security schemes:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

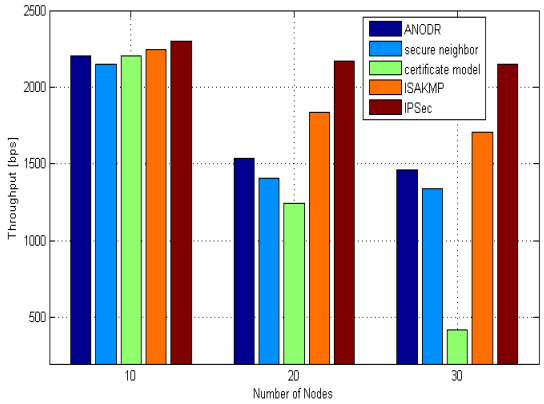

Fig.2- Throughput

The above graph shows the variation in the throughput of different security schemes. In this, 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, HMAC-SHA algorithm for certificate generation and authentication. In ANODR, ISAKMP and secure neighbour model schemes there is also degradation in throughput with increase in number of nodes.

B. End-to-end Delay

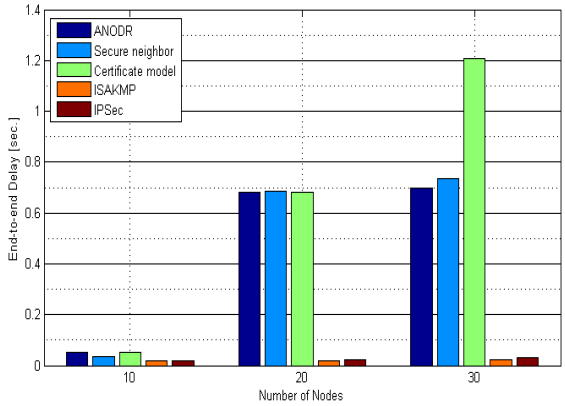

Fig3. End-to-end Delay

The above graph shows the variation in the end-to-end delay of different security schemes in wireless sensor network. The asymmetric cryptographic schemes have higher end-to-end delay than symmetric key cryptographic schemes. The public key cryptography schemes acquire more storage space because of large size. It require much time for processing 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. In this RSA public key algorithm is used for certificate creation. The symmetric key cryptography based security schemes had less delay like ISAKMP has very less end-to-end delay as compared to other schemes.

C. Energy Consumed in Transmit mode

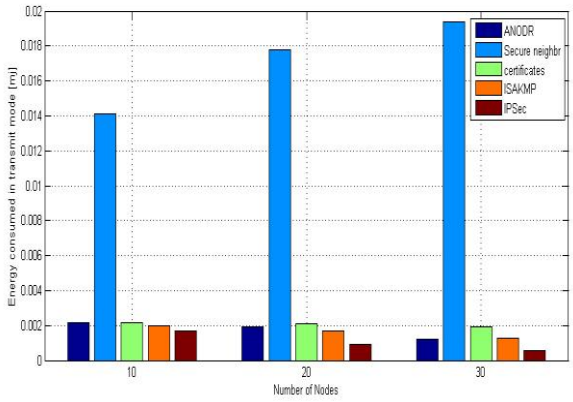

Fig.4- Energy Consumed in transmit mode

This graph shows the variation in the energy consumption of different security schemes in transmit mode. In this, the secure neighbor model consumed 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 ISAKMP security schemes also consumed less energy as number of nodes increases than other asymmetric key cryptographic based schemes.

D. Energy Consumed in Receive mode

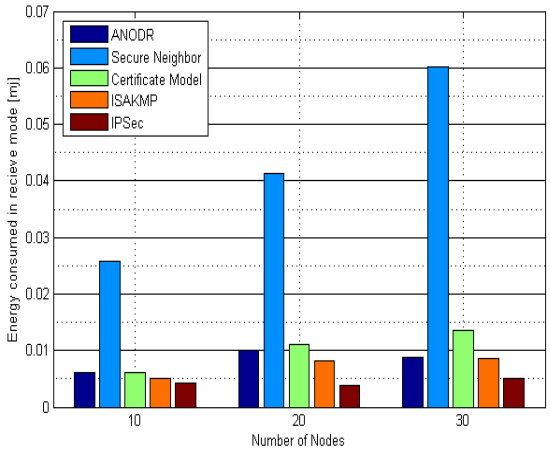

Fig.5- Energy consumed in receive mode

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

This graph shows the variation of energy consumption of different security schemes in receive mode. In this the secure neighbour model consumed more energy in receive modes as compared to other security schemes and it further increases with scalability. The IPsec security scheme again consumed less amount of energy as compared to other security schemes. The energy consumption rises with slow rate rather than other security schemes. It's considered as best in this case.

VI. CONCLUSION AND FUTURE WORK

In this paper, we present different security schemes based on symmetric and asymmetric key cryptography and how they affect the Quality of service. QoS of wireless sensor network is investigated on the basis of metrics like throughput, end-to-end delay 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 appropriate cryptographic methods depends on the processing capability of the sensor nodes characterized by the constraints on energy, computation capability, 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 WSN's. The asymmetric key cryptographic schemes affect the QoS of WSN's more than symmetric key cryptographic schemes. We have concluded from the simulation that the throughput of symmetric key schemes is more as compared to asymmetric key cryptographic schemes. It is 4919 bits per sec. more than that of asymmetric key schemes as shown in fig.2. The throughput of IPSec symmetric key schemes is more than others schemes. 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 also more than symmetric key based security schemes. The certificate model scheme has higher delay than all other schemes and it increases rapidly with increase in the number of nodes. The symmetric key based scheme namely ISAKMP has very less delay among all cryptographic schemes. The asymmetric key cryptographic schemes require more time for their processing. The end-to-end delay of symmetric key based schemes is 0.62796 seconds less than asymmetric key based cryptographic schemes as shown in fig.3. The end-to-end delay of IPSec schemes is also close to ISAKMP scheme.

The energy consumption of symmetric key based schemes is less as compared to asymmetric key cryptographic schemes. The symmetric key based scheme named IPSec consumed less amount of energy both in energy transmit and receive mode. For energy consumed in transmit mode, it consumes 0.0160516mj less amount of energy as shown in fig.4 and for energy consumed in receive mode, it consumes 0.037991mj less amount of energy than asymmetric key based security schemes as shown in fig.5.

The QOS of symmetric key based cryptographic schemes are better than asymmetric key based schemes for wireless sensor network. The IPSec symmetric key based schemes has high QOS than other cryptographic schemes.
The future work includes the analysis of symmetric key cryptographic schemes under different attacks.

REFERENCES

[1] H.C. Chaudhari, L.U. Kadam, "Wireless Sensor Networks: Security, Attacks and Challenges", *International Journal of Networking*, Volume 1, 2011.
[2] J. Jeong, X. F. Jiang, D. E. Culler, "Design and Analysis of Micro-Solar Power Systems for Wireless Sensor Networks", *Electrical Engineering and Computer Sciences, University of California at Berkeley*, 2007.
[3] David Boyle, Thomas Newe, "Securing Wireless Sensor Networks:Security Architectures", *Journal of networks*, Vol. 3, 2008.
[4] Mariano Garcıa Otero, Adrian Poblacion-Hernandez, "Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques", *International Journal of Distributed Sensor Networks*, 2012.
[5] D.Devi Aurna, P.Subashini,Phd, SNAuth-SPMAODV:" Secure Neighbor Authentication Strict Priority Multipath AODV against Denial of Serviceattack for MANET in Military Scenario", *International Journal of Computer Applications* , 2012.
[6] Dr.G.Padmavathi1, Dr.P.Subashini, Ms.D.Devi Aruna, "DSSS with ISAKMP Key Management Protocol to Secure Physical Layer for Mobile Adhoc Network", *International Journal of Network Security & Its Applications (IJNSA)*, 2012.
[7] Atul Kahate, "Cryptography and network security", *The Tata Mcgraw- hill*, 2003.
[8] Jiejun Kong, Xiaoyan Hong," ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks", *ACM*, 2004.
[9] T.Kavitha, D.Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey", *Journal of Information Assurance and Security*, 2010.
[10] Jaydip Sen, "A Survey on Wireless Sensor Network Security", *International Journal of Communication Networks and Information Security* vol. 1, 2009.
[11] Shahid Raza, Tony Chung, Simon Duquennoy, Dogan Yazar, Thiemo Voigt, Utz Roedig, "Securing Internet of Things with Lightweight IPsec", *SICS*, 2011.
[12] Jorge Granjal, Ricardo Silva, Edmundo Monteiro, Jorge Sa Silva, Fernando Boavida, "Why is IPSec a viable option for Wireless Sensor Networks", *IEEE*, 2008.
[13] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", *IJCIT* vol.2, 2011.
[14] M. Johnson, M. Healy, P. van de Ven, M. Hayes, J. Nelson, T. Newe, E. Lewis, "A Comparative Review of Wireless Sensor Network Mote Technologies", *IEEE Sensors* 2009.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

BIOGRAPHIES

Gurjot Singh is presently pursuing M.TECH in CSE(E-Security) from BBSBEC,Fatehgarh Sahib, Punjab, India. His research includes cryptographic schemes in wireless sensor network.

Er. Sandeep Kaur Dhanda is currently serving as Assistant Professor in Computer Science and Engineering. Her research includes parallel computing.

.