Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Symmetric key Cryptographic Protocol IPSec to Prevent Wormhole attack in Wireless Sensor Network

Er. Gurjot Singh*
CSE/IT Department, BBSBEC
Fatehgarh Sahib, Punjab, India

Er. Sandeep Kaur Dhanda
Asstt. Prof., CSE/IT Dept., BBSBEC
Fatehgarh Sahib, Punjab, India

Abstract— Wireless sensor network are usually deployed in unattended or hostile environment for information gathering and transmitting it to the base station for evaluation. Due to inheritance limitations of sensors, security is the major issue in WSN. WSNs are susceptible to various critical external and internal attacks being limited by computation resources, bounded memory capacity and battery life, processing power, lack of tamper resistant packaging and the use of insecure wireless communication channels. The wormhole attack is one of the severe attack on WSN that can effect the networks performance. In this, attackers create a low-latency link between two points in the network. The wormhole attack tunnels the packets from one end to another end by modifying or altering its content. In this paper, the IPSec (Internet protocol security) protocol that is based on symmetric key cryptography is implied against wormhole attack in WSN. IPSec provides data security at the IP packet level. It provides end-to end security. IPSec helps to create authenticated and confidential packets for IP layer. IPSec uses two efficient protocols i.e. AH (Authentication Header), ESP (Encapsulating Security Protocol). Each has their own responsibility and functionality. These protocols are operating in two basic modes that are: Transport Mode and Tunnel Mode. In the present work, ESP protocol is used in transport mode in wireless sensor network. It operates on DES-CBC algorithms for encryption/decryption and HMAC-MD5 algorithms are used for authentication. The performance of IPSec protocol is evaluated on the basis of metrics like throughput, packet received, end-to-end delay and jitter.

Keywords— IPSec, Wormhole attack, WSN, AH and ESP

I. INTRODUCTION

Wireless sensor networks have appeared as one of the emerging technologies that combines sensing, computing and wireless networking into tiny embedded devices named sensor nodes. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna that connected to an external antenna, micro-controller and an electronic circuit for interfacing with the sensors and an energy source i.e. battery. Consider the Crossbow "MICAz" mote, a typical mote used in WSNs [1]. It consists of a battery, 4Mhz- 8Mhz micro-controller, microprocessor (Atmega128), RF transceiver, ADC, 128K bytes Program Flash Memory and 4K bytes EEPROM, 48-256kB of instruction memory [2]. Berkeley's MICA2 possess 4-8 MHz, 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency [3].

The early research on WSNs has mainly focused on monitoring applications, such as agriculture [4] and environmental monitoring [5], based on low-rate data collection, current WSN applications can support more complex operations ranging from health care [6] to industrial monitoring and automation [7]. Besides these, the availability of low-cost hardware and rapid development of tiny cameras and microphones have enabled a new class of WSNs: multimedia or visual wireless sensor networks. Due to limited constraints of sensor devices, security is the major issue in WSN. Wireless sensor networks are susceptible to wide range of various critical external and internal attacks being limited by computation resources, bounded memory capacity and battery life, processing power, lack of tamper resistant packaging and the use of insecure wireless communication channels. To design a completely secure WSN, security must be integrated in each node of the system [1]. Any component of a network implemented without any security could easily become a point of attack [8]. Although many security protocols and algorithms have been proposed for traditional wireless and ad hoc networks, many of them are not well suited to WSNs. It is therefore important to analyse the feasibility of applying security mechanisms or architectures designed for other contexts to WSNs [9]. Conventional networks require protection against eavesdropping, injection or modification of propagated data packets. Most of the WSN`s applications require that level of protection. Cryptography is the standard method of defence against such attacks [8]. Varying levels of cryptographic protection implies a varying level of overheads in the form of increased packet size, code size, processor usage 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. Thus, effective approach is to use more efficient symmetric cryptographic alternatives [10]. 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 [11].

II. ATTACK ON WIRELESS SENSOR NETWORK

Wireless sensor networks are susceptible to wide range of security attacks due to multi chip nature of the transmission medium i.e. wireless medium and the random deployment of sensor nodes in unprotected or hostile environment. There is no standard architecture of communication protocol in WSNs and the limited constraints lead it to the security vulnerabilities i.e. severe attacks. There are different types of attacks on different layers of the network. Several attacks on network layer or routing attacks are as black hole, grey hole, wormhole, sink-hole, selective forwarding, hello flood, acknowledgement flooding, false routing and other severe attacks [9].

A. Wormhole attack in WSN`s

Scarcity of various resources makes wireless sensor network vulnerable to several kinds of severe attacks. The attacker possessing sufficiently large amount of memory space, power supply, processing abilities and capacity for high radio transmission, results in generation of several malicious attacks in the network [12]. Wormhole attack is a typically a denial of service attack that misleads routing operations even without the knowledge of encryptions methods. These characteristics make it very important to identify and to defend against it [13]. Wormhole attack is a severe attack on wireless sensor network routing where two or more attackers are connected by high speed off-channel link called wormhole link [13]. Wormhole attack exits in two different modes called hidden and exposed mode, depending on whether attackers put their identity into packet headers when tunnelling and replying packets [14].

In wormhole attack, a pair of attackers forms tunnels to transfer data packets and reply them into the network [15]. This attack has tremendous effect on wireless networks, especially against routing data/ information. The tunnel is formed between the two colluding attackers is referred as wormhole.

- **Types of Wormhole Attack**

The number of nodes involved in establishing and the way through which it establishes the wormhole is classified as follow:

- **Wormhole using Out-of-Band Channel**- In this, two-ended wormhole i.e. a specified out-of-band high bandwidth channel is placed between the end points to create a wormhole link in particular network [16].
- **Wormhole using Packet Encapsulation-** In a network, each packet is routed through the legitimate path only. When the packets are received by the wormhole end it get encapsulated to prevent nodes on way from incrementing hop counts. The packet is brought into original form by the second end point [12].
- **Wormhole using High Power Transmission-** This kind of wormhole approach has only one malicious node with much high transmission capability that attracts the packets to follow path passing from it.
- **Wormhole using Packet Relay-** In this, only one malicious node is sufficient for replays the data packets between two far nodes and this way the fake neighbours are created in the network [16].

III. INTERNET PROTOCOL SECURITY (IPSEC)

IPSec is a set of protocols suite "designed to provide interoperable, high quality, cryptographic-based security for the network" [1]. The services like data integrity, access control, authentication and confidentiality i.e. encryption and replay protection of IP layer as well as the layers above it are provided by IPSec. It could protect one or more paths between two pairs of hosts, between a pair of security gateways (a security gateway is an intermediate element that implements IPSec), or between a host and a security gateway (SG) [1]. The administrator provides security services for different purposes like it is possible to create a single tunnel (IP encapsulation) for all TCP connections in between two hosts and specified tunnels for each of the connections. The key concept behind this idea is called a Security Association (SA). The SA is identified by a unique Security Parameter Index (SPI), an IP destination address and a security protocol (Authentication Header or Encapsulating Security Payload) [22].

Authentication Header (AH) and Encapsulating Security Payload (ESP) are secure protocols provided by IPSec to form SAs [15, 17]. The AH provides connectionless integrity, data authentication and an optional anti-replay service. The ESP provides confidentiality and limited traffic flow confidentiality and the services provided by the AH too. These protocols can be used alone or in combination. Each protocol supports two modes of use: transport mode and tunnel mode. These are the security associations to be used. First provides protection primarily for upper layer protocols, while the other is used to encapsulate IP packets. Transport Mode protects packets coming from transport layer to network layer by encapsulating the payload. It does not encapsulate the header. Tunnel mode is used when communication occurs between two routers, a router and host or between a host and a router. Each SA defines the algorithms for encryption/ decryption, authentication, hash and key exchange for protecting a particular path and the data packets.

A. Encryption Algorithms

The encryption algorithm employed is specified by the Security Association. ESP is designed to use with symmetric encryption algorithms. The IP packets may arrive out of order and each packet must carry some data that allows the receiver to establish cryptographic association for decryption. This data may be carried in the payload field or derived from the packet header [17]. The ESP protocol makes provision for padding of the plaintext so the encryption algorithms employed with ESP may exhibit either block or stream mode characteristics. In the present work DES-CBC algorithm is used for encryption/ decryption. DES is a cipher block. It encrypts data in block, each of size 64 bits. That is, the plain text of size 64 bits goes as the input to DES, which produces 64 bits of cipher text. It uses 56 bit key size for encryption/ decryption of the plain text to cipher text.

B. Authentication Algorithms

The authentication algorithm employed for the ICV computation is specified by the Security Association. For the point-to-point communication, efficient authentication algorithms include [17] Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g., DES) or on one-way hash functions (e.g., MD5 or SHA-1) are implied. In the present work, for authentication purposes HMAC- MD5 algorithm is used.

IV. RELATED WORK

Boyle and Newe [8] had mentioned various security schemes. They concluded that the Symmetric key cryptography based architectures have been the main source of security in Wireless Sensor Networking to date. There is much research available claiming that Public Key based solutions will provide better solutions, based on smaller key sizes and less storage requirements (under ECC), for more secure communications, also even providing superior energy efficiency. They concluded from an authentication perspective, the CBC-MAC algorithm is the most popular method of providing authentication for symmetric key based algorithms. Chaudhari and Kadam [3] had summarised the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The schemes Key establishment and trust setup, Secrecy and Authentication, Secure group management, Intrusion detection are discussed.

Garcıa-Otero and Poblacion-Hernandez [18] had presented a minimalist model for a wormhole attack to a WSN that can be effectively counteracted by two different detection procedures, based on the underlying ideas of RSS-based range-free localisation methods. The first one (DWARFLoc) operates simultaneously with the localisation procedure, and the second one (DWARF Test) is a post localization detector that tries to validate a posteriori the estimated node position. Simulations suggest that DWARF Test has much better detection performance than DWARFLoc but requires more transmissions to be carried out.

Raza et al. [19] had described the specification of IPsec for 6LoWPAN. Further more we have presented an implementation of IPsec for 6LowPAN and we have demonstrated that it is possible and feasible to use this mechanism to secure communication between sensor nodes and hosts in the Internet.

Aggarwal et al. [20] had discussed the routing protocols and different security attacks. They consider the wormhole attack as routing attack and compare the wormhole attack on AODV and DYMO manet routing protocols. They evaluate that AODV protocol was more effected than DYMO protocol when nodes are mobility. Due to this AODV is better than DYMO. Wormhole attack degrades the performance of two routing protocols. So the trustworthy techniques that will detect and prevent the wormhole attack are used.

Karuppiah et al. [21] had discussed the simple novel technique to detect malicious wormhole nodes. The proposed methodology when each node is in metric and when there are sudden changes in the traffic to detect a wormhole. This is done by setting counter values in sensor nodes. Wormhole attack is notice by improve the power consumption for each and every sensor nodes. They have evaluated the result that when saving in power consumption of wireless sensor network is 5 percent which is considered as greatest reduction in wireless sensor network.

V. SIMULATION DETAILS

QualNet 4.5.1 Network Simulator tool is used to evaluate the performance of 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 wormhole attack is implemented on random number of node in network. The security schemes IPsec is implemented on sensor network against wormhole attack. The performance is measured on the basis of metrics like throughput, end-to-end delay, total packet receive and jitter. The simulation time is run for 200 second. For simulation, the different parameters set are shown in table 1:

TABLE 1. 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	50
Routing Protocol	AODV
Attack	Wormhole attack (Threshold)
Security Schemes	IPSec
Traffic Type	CBR
Energy Model	Micaz
Mobility Model	Random Waypoint
Device type	PAN coordinator, FFD and RFD

A. Simulation Scenario Design

The nodes are placed randomly on terrain of size 1000* 1000m. There are total 50 nodes placed on terrain. One wireless cloud is placed on the terrain has configured to 802.15.4 network. All the nodes are link wirelessly with the wireless subnet cloud except the two nodes named 20 and 21 as shown in figure 1. The nodes 20 and 21 are link to other wireless subnet cloud that has configured to wormhole attack. The nodes are made mobile nodes that move randomly on the terrain. CBR is used as data traffic application with multiple source and destination. Then different security scheme IPSec is configured on all the nodes and simulation is run for 200 seconds i.e the simulation time.

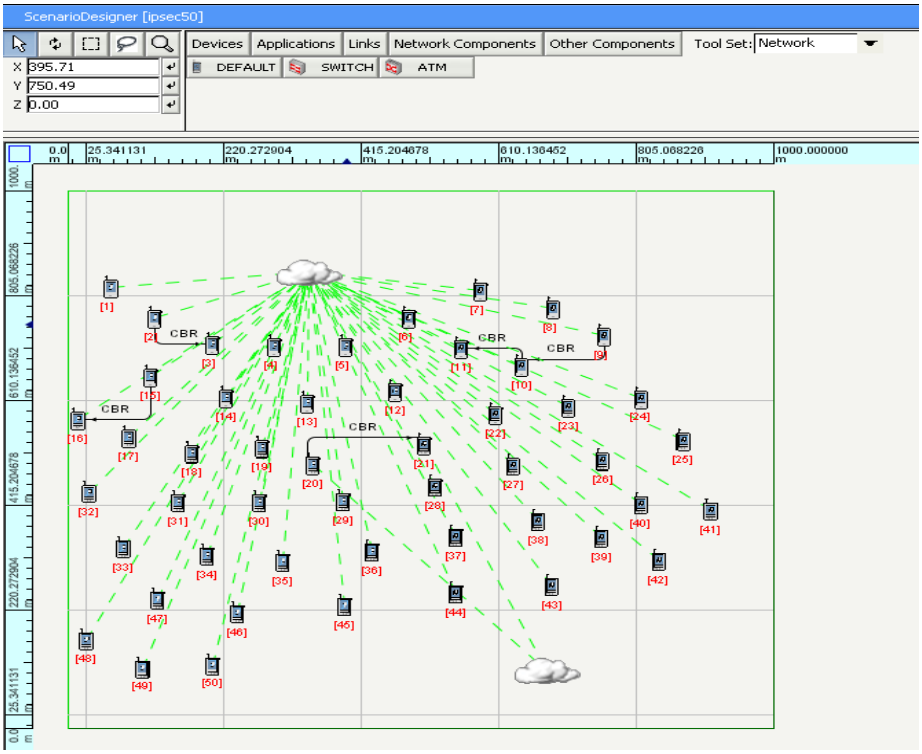

Fig 1 Scenario Design

VI. EXPERIMENTAL RESULT AND EVALUATION

This section evaluates the performance of IPSec protocol against wormhole attack in wireless sensor network. After describing our implementation and simulation setup, it has been evaluated, how IPSec prevents the wormhole attack in WSNs. The performance is evaluates on the basis of metrics like throughput, end-to-end delay, jitter and total packet received.

A. Throughput (bits/sec.)- The graph shows the value of throughput of wireless sensor network. The value of throughput is 2295 bits/sec i.e. the (without IPSec) value when the network is under wormhole attack as shown in figure 2. When cryptographic based scheme i.e. IPSec is implement on WSN to prevent it against that severe attack then the value of throughput increases i.e. 2322.5 bits/sec. The network is considered as efficient if it throughput is high and delay is less.

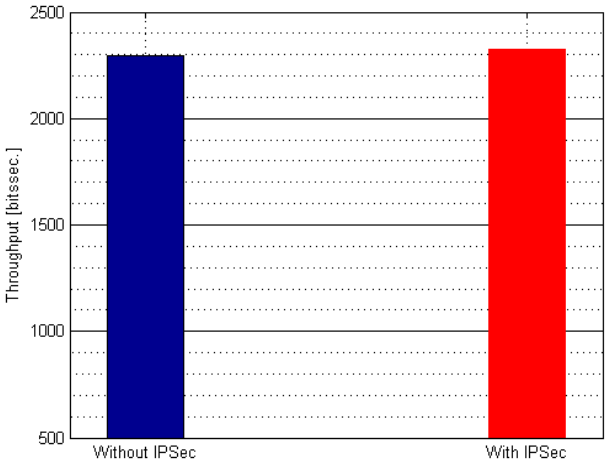

Fig. 2 Throughput

B. End-to-end delay (sec.) -The graph shows the value of end-to-end delay of WSNs. The value of end-to-end delay is 0.035072407 sec. i.e. the (without IPSec) value under wormhole attack as shown in figure 3 and when IPSec protocol i.e. cryptographic based scheme is applied to WSN to prevent it from wormhole attack the value of end-to-end delay decreases i.e. 0.020055154 sec. as shown in figure 3.

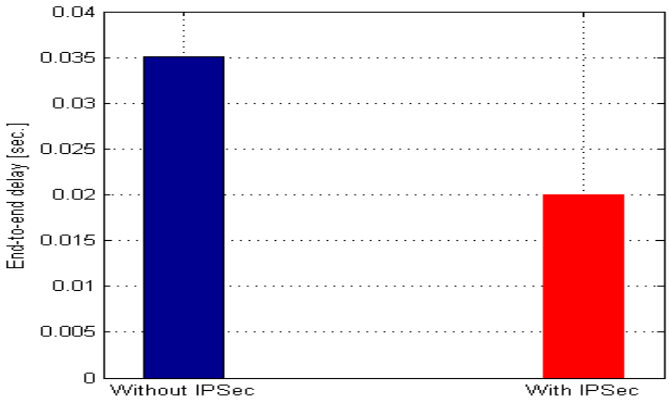

Fig 3 End-to-end delay

C. Jitter (sec.) -The graph shows the value of jitter of wireless sensor network under wormhole attack i.e. without IPSec value and with IPSec value. The value of jitter is 0.006050152 sec. under wormhole attack as shown in figure 4 and when IPSec protocol i.e. cryptographic based scheme is applied to it to prevent it from wormhole attack the value is less i.e. 0.001003508 sec. as shown in figure 4. The network is considered to be efficient and reliable if its jitter as well as the packet drop ratio is less**.**

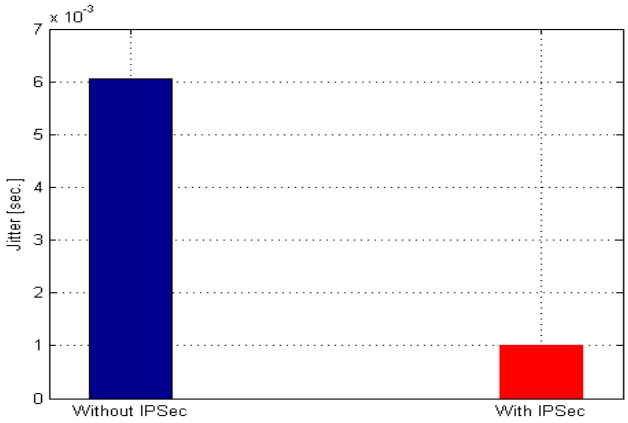

Fig 4 Jitter

D. Total packet received -The graph shows the value of total packet received by nodes or receivers in wireless sensor network. The total packets that are sent in the network are 48. The total packet received when wormhole attack is encountered on WSN are 33 out of 48 as shown in figure 5 and when IPSec protocol is applied to wireless sensor network to prevent it from that severe attack the value of total packet received is increased to 43 as shown in figure 5. The packet loss rate is less when IPSec is applied to wireless sensor network as compared to under attack.

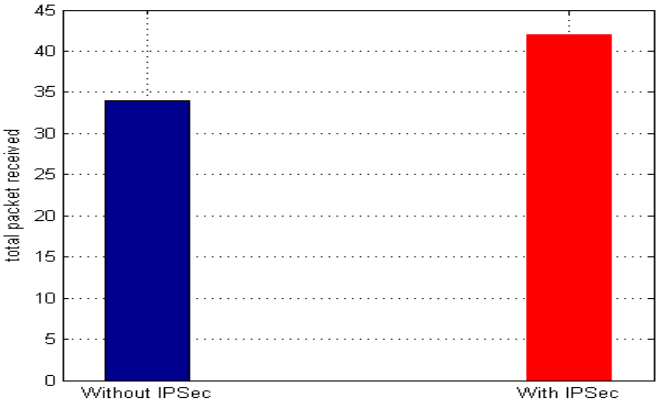

Fig 5 Total packet Received

VII. CONCLUSION

In this paper, the prevention of wormhole attack in wireless sensor network using cryptographic scheme i.e. IPSec is presented and the result is evaluated on the basis of metrics like throughput, end-to-end delay, total packet received and jitter. The symmetric key cryptography based schemes have been the main source of security in Wireless Sensor Network, to date. The selection of the appropriate cryptographic scheme depends on the processing capability of the sensor nodes characterised by the limited constraints such as its energy, computation capability, low 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. It is concluded that, the throughput of wireless sensor network increased when security scheme in implied on it. The network is considered as efficient when the throughput of the network is high and the end-to-end delay is less. The end-to-end delay and the jitter of wireless sensor network decreases with cryptographic schemes implied on it as shown in figure 3 and 4. The total packet received in the network is increased i.e. the packet loss rate decreases as shown in figure 5. Finally it is concluded that the IPSec protocol can effectively prevent the wormhole attack in wireless sensor network.

REFERENCES

[1] S. Kent, R. Atkinson. Security Architecture for the Internet Protocol, Internet Request for Comments RFC 2401. 1998.

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

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

[4] T. Wark, P. Corke, P. Sikka, L. Klingbeil, Y. Guo, C. Crossman, P. Valencia, D. Swain and G. Bishop-Hurley, "Transforming agriculture through pervasive wireless sensor networks", IEEE Pervasive Computing 6 (2) pp. 50-57, 2007.

[5] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk and J. Anderson, "Wireless sensor networks for habitat monitoring, in: WSNA'02". Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, ACM, New York, NY, USA, pp. 88–97, 2002.

[6] A. Milenkovic, C. Otto and E. Jovanov, "Wireless sensor networks for personal health monitoring: issues and an implementation", Computer Communications 29 (13–14) pp. 2521–2533, 2006.

[7] V. Gungor and G. Hancke, "Industrial wireless sensor networks: challenges, design principles, and technical approaches", IEEE Transactions on Industrial Electronics 56 (10) pp. 4258–4265, 2009.

[8] Boyle David and Newe Thomas, "Securing Wireless Sensor Networks: Security Architectures", Journal of networks, Vol. 3, No. 1, pp. 65-77, 2008.

[9] Jorge Granjal, Ricardo Silva, Edmundo Monteiro, Jorge Sa Silva and Fernando Boavida, 2008. "Why is IPSec a viable option for Wireless Sensor Networks" IEEE, pp. 802- 807, 2008.

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

[11] 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.

[12] Gurpreet Kaur and Sandeep Kaur Dhanda, "Analyzing the effect of wormhole attack on routing protocols in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue. 8, pp. 3217- 3223, 2013.

[13] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", computer networks (Elsevier),vol. 52, pp. 2292- 2330, 2008.

[14] Murthy Siva ram C. and Manoj B.S. ,"Performance Simulation of Multihop Routing Algorithms for Ad-Hoc Wireless Sensor Networks Using NS2", In proceeding in 10th International Conference on Advanced Communication Technology.

[15]. S. Kent, R. Atkinson. IP Authentication Header. Internet Request for Comments RFC 2402, 1998.

[16] Majid Meghdadi, Suat Ozdemir and Inan Guler, "A survey of wormhole based Attacks and their countermeasures in Wireless Sensor Networks" , IETE Technical Review, VOL.28, 2011.

[17] S. Kent, R. Atkinson. IP Encapsulating Security Payload (ESP). Internet Request for Comments RFC 2406, 1998.

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

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

[20] Richa Agrawal, Rajeev Tripathi and Sudarshan Tiwari, "Performance comparison of AODV and DYMO MANET Protocols under Wormhole Attack Environment", International Journal of Computer Applications, Vol. 44, 2012.

[21] A. Babu Karuppiah, Vidhya G. Sri and S. Rajaram, "Energy Efficient Wormhole Detection Technique by Traffic Analysis in Wireless Sensor Networks", International Journal Of Engineering And Computer Science, Volume 2, 2013.

[22] Manju, Ranjana Thalore, Jyoti and M.K Jha, "Performance Evaluation of Bellman-Ford, AODV, DSR and DYMO Protocols using QualNet in 1000m×1000m Terrain Area", International Journal of Soft Computing and Engineering, volume-2, 2013.

