ISSN No. 0976-5697

Volume 4, No. 11, Nov-Dec 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Prevention of Blackhole Attack in Wireless Sensor Network using IPSec Protocol

Gurjot Singh
Computer Science and Engineering department
Baba Banda Singh Bahadur Engineering College
Fatehgarh Sahib, Punjab, India
Gurjotsingh52@yahoo.com

Jagdeep Singh
Computer Science and Engineering department
Guru Nanak Dev Engineering College
Ludhiana, Punjab, India
jagdeepmalhi@gndec.ac.in

Abstract: A Wireless Sensor Network is consist of spatially distributed autonomous sensor devices to cooperatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure and pollutants etc. at various locations. WSN is highly prone to severe attacks and conventional techniques against these attacks are not desirable due to the resource constrained nature of the sensor devices i.e. low battery power, limited computation capability, bounded memory and energy resources, susceptibility to physical threat and the use of insecure wireless communication channels. Sensor nodes communicate via wireless links over limited frequency and bandwidth. However, there are still a lot of unresolved issues in wireless sensor networks of which security is one of the hottest research issues. The black-hole attack is one of the severe deniel-of-servie attack on wireless sensor network can be accomplished by dropping the data packets. The attack can be accomplished either selectively i.e. by dropping data packets for a particular destination or a randomly selected portion of the data packets or by dropping all the data packets in that network. In this paper, the IPSec (Internet protocol security) protocol based on symmetric key cryptography is used against black-hole attack in WSN. IPSec provides data security at the IP packet level. 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 specifications and functions. 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. 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, total packet received, end-to-end delay and jitter.

Keywords: Black-hole attack, IPSec, WSN, AODV, CBR

I. INTRODUCTION

Advances in wireless communications have enabled the development of low-cost and low power wireless sensor networks (WSNs) [1]. WSNs have many potential applications [1, 2] and unique challenges. A WSN is a heterogeneous system consists of hundreds or thousands low-cost and low-power tiny sensors to monitoring and gathering information from deployment environment in real-time [3, 4, 5]. Common functions of WSNs include broadcasting, multi-casting, routing, forwarding the data packets and route maintenance in the network. The sensor's components composed of: sensor unit, processing unit, storage/memory unit, power supply unit and wireless radio transceiver. These components/units are communicating to each other. The existing components on WSN's architecture are including sensor nodes (motes or field devices that are sensing data), network manager, security manager, aggregation points, base stations (access point or gateway) and user interface.

Besides, there are two approaches in WSN's communication models containing hierarchical WSN versus distributed [3] and homogeneous WSN versus heterogeneous [3]. WSNs are vulnerable to many types of attacks such as physical attacks, network attacks. They are one of the most malicious and harmful/severe attacks on WSNs. Due to unsafe, unattended and unprotected nature of communication channel [7, 6, 8], untrusted and unsafe broadcast transmission media, deployment in hostile environments [1, 2], automated nature and limited resources, the most of security techniques of traditional networks are impossible in WSNs; therefore, security is a main and complex requirement for these networks, especially against to the network attacks. It is necessary to design more secure mechanism for these networks [2, 3], which attending to be WSN's constraint and it should cover different security related aspects of WSNs that includes confidentiality, integrity, availability and authenticity.

A. Security in WSNs:

The intrusion detection techniques in WSNs are in growth in today`s world but there are many methods to disrupt these networks. In WSNs, data accuracy and network health are necessary; because these networks usually use on confidential and sensitive environments. There are three security key points on WSNs, including system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality). The security issues in WSNs are as:

a. Key establishment,
b. Secrecy,
c. Authentication,
d. Privacy,
e. Robustness to DoS attacks,
f. Secure routing, node capture [9, 10];

II. ATTACKS ON WSNS

Wireless sensor networks are susceptible to wide range of security attacks due to multichip nature of the transmission medium i.e. wireless medium and the limited constraints like energy, storage and computation power. There are different types of attacks on different layers of the network. Several attacks on network layer or routing attacks are as wormhole, sinkhole, selective forwarding, hello flood, acknowledgement flooding and false routing attacks. The

© 2010, IJARCS All Rights Reserved

black hole attack is one of the severe attack on WSNs that is described as:

A. Black hole attack:

A black hole attack is an attack that is mounted by an external adversary on a subset of the sensor nodes (SNs) in the network. The adversary captures these nodes and reprograms them so that they do not transmit any data packets, namely the packets they generate and the packets from other sensor nodes that they are supposed to forward. The malicious node starts advertising very attractive routes to data sink. The neighbor nodes of that malicious node select it as the next hop for forwarding the messages and considering it a high quality route. The neighboring nodes propagate this route to other nodes for communication. Thus all the network traffic get attracted to the malicious node that can either drop it, selectively forward it based on some malicious filtering mechanism or change the content of the messages before relaying it. This malicious node has thus formed a sink hole with itself at the center. The sink hole is characterized by intense resource contention among neighboring nodes of the malicious node for the bounded bandwidth, frequency and channel access [12]. This results in congestion and can accelerate the energy consumption of the nodes involved in the network that leads to the formation of routing holes due to nodes failure. With this several other types of denial of service attacks are then possible on the sensor network [11, 12].

III. INTERNET PROTOCOL SECURITY (IPSEC)

IPSec is a set of protocols suite "designed to provide inter operable, high quality, cryptographic-based security for the network" [13]. IPSec security association protects the connection between the communicating parties with cryptographic methods. Associated with each end of the SA is cryptographic key and other information such as the identity of the other end, the sequence number currently being used and the cryptographic services being used i.e. Integrity only, or encryption + integrity and which cryptographic algorithms should be used. The SA is considered as unidirectional, so a conversation between two parties will consist of two SA`s one in each direction. The IPSe header includes a field called SPI (security parameter index), which identifies the security association [14].

AH and ESP are the two types of IPSec headers. AH provides integrity protection only. ESP provides encryption and integrity protection. The integrity protection provided by Esp and AH is not identical.

The IPSec specification talks of two modes of applying IPSec protection to a data packet. Transport mode refers to adding the IPSec information between the IP header and the remainder of the packet. Tunnel mode refers to keeping the original IP packet intact and adding a new IP header and IPSec information outside. Transport mode is more logical when IPSec is being applied end-to-end [15].

In the present work, ESP is used for both encryption and integrity protection. 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 uses 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. ESP authentication provides authentication and integrity for the payload and not for the IP header. In this, 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. For authentication HMA- MD5 algorithm is used based on symmetric encryption algorithms (e.g., DES) or on one-way hash functions.

IV. RELEATED WORK

Boyle and Newe [16] 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 [17] had summarized 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.

Raza et al. [18] 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.

Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M. [19] had proposed a appproach for secure routing algorithm against black hole attacks for wireless sensor networks. Delivering data to the base station is more important especially in the case of real time applications for which it is designed. By having several base statio we make sure that the data is being delivered to the destination base station despite the presence of black-hole regions near the neighborhood of the sensor nodes near the base stations. This ensures the data delivery and security of the data delivered can be taken are of by using enryption algorithms.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto [20] had proposed an anomaly detection scheme using dynamo training method in which the training data is updated at regular time intervals. Through the simulation their method shows significant effectiveness in detecting the black-hole attack.

Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad [21] had described all the existing defensive schemes according to their best of knowledge against this attack along with their drawbacks, thus providing researchers a better understanding of the attack and current solution space. Their paper also classifies

© 2010, IJARCS All Rights Reserved

proposed schemes according to their nature and defense. Nature of scheme classifies into Distributed and Centralized. Defense of scheme classifies into detection and prevention.

Nadeem Ahmed, Salil S. Kanhere and Sanjay Jha [22] had presented different types of holes, discuss their characteristics and study their effects on successful working of a sensor network. They presented a state-of-the-art in research for addressing the holes related problems in wireless sensor networks and discuss the relative strengths and shortcomings of the proposed solutions for combating different kinds of holes.

Chris Karlof and David Wagner [23] had proposed security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks-sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. We describe crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.

V. SIMULATION DETAILS

QualNet 4.5.1 Network Simulator tool is used to evaluate the performance of IPSec cryptographic scheme against black-hole attack 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. 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 black-hole attack is implemented on random number of node in network. The security schemes IPsec is implemented on sensor network against black-hole attack. The performance is measured on the basis of metrics like throughput, end-to-end delay, packet received and jitter. The simulation time is 200 second. For simulation the different parameters are 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
No. of Nodes	50
Routing Protocol	AODV
Attack	Black-hole attack
Security protocol	IPSec
Traffic Type	CBR traffic
Energy Model	Micaz
Mobility Model	Random Waypoint mobility
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. 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 have configure to blackhole attack setting. 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 IPSec protocol is configured on all the nodes and simulation is run for 200 seconds i.e the simulation time. The working of simulation is shown in figure 2.

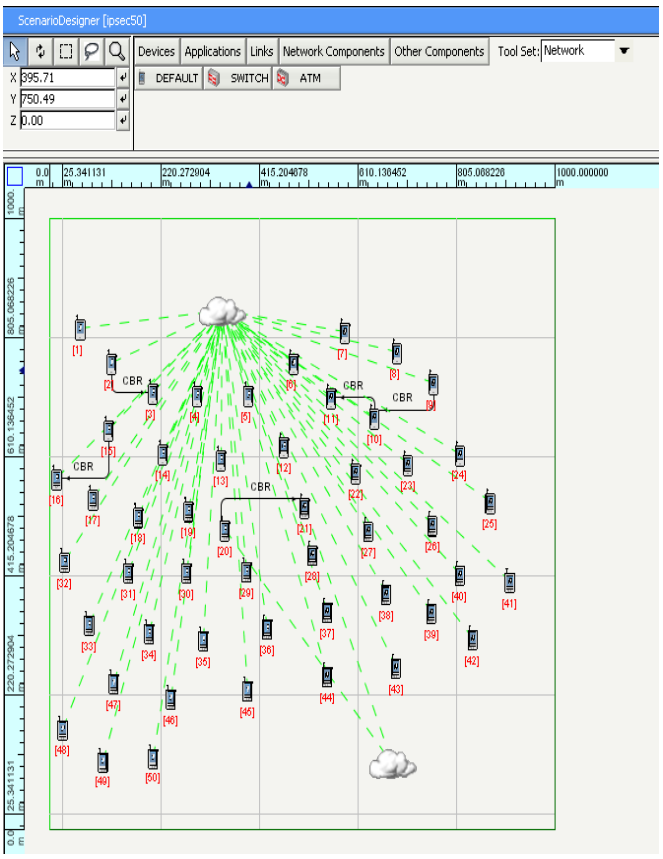

Figure 1. Scenario Design

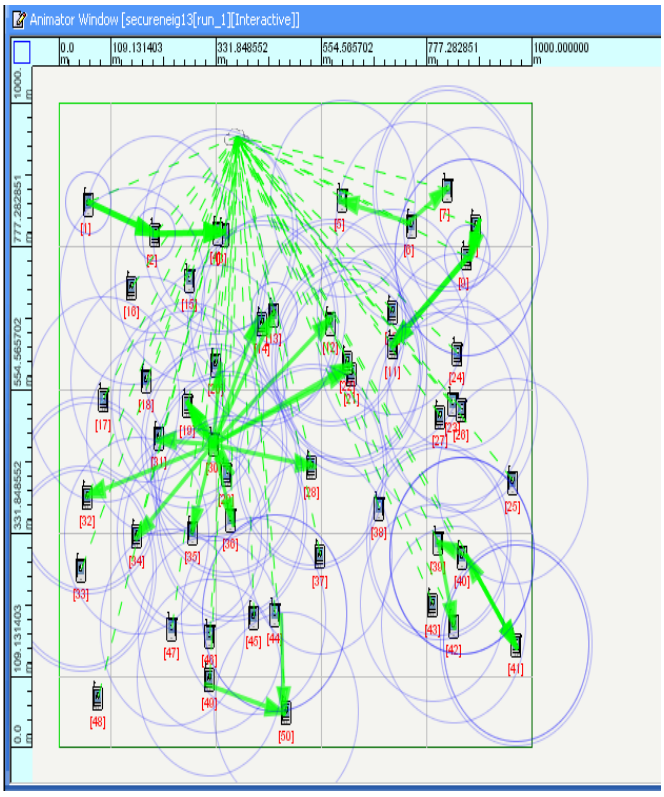

Figure 2. Working of simulation scenario

© 2010, IJARCS All Rights Reserved

VI. RESULT AND DISCUSSION

This section evaluates the performance of IPSec protocol against black-hole attack in wireless sensor network. After describing our implementation and simulation setup, it has been evaluate how IPSec prevents the black-hole 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.):

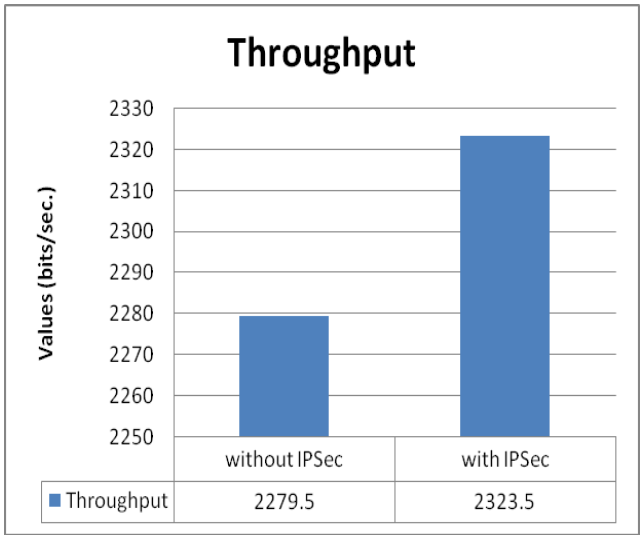

Figure 3. Throughput

The above graph shows the value of throughput in WSNs. It is defined as the number of packets or bits delivered per second to the destination. The value of throughput is 2279.5 bits/sec. under black-hole attack and when cryptographic security i.e. IPSec is implemented on the network to defend against black-hole attack then the throughput become increased to 2323.5 bits/sec. as shown in figure 3. The network is considered as efficient if it throughput is high and delay is less.

B. End-to-end Delay (sec.):

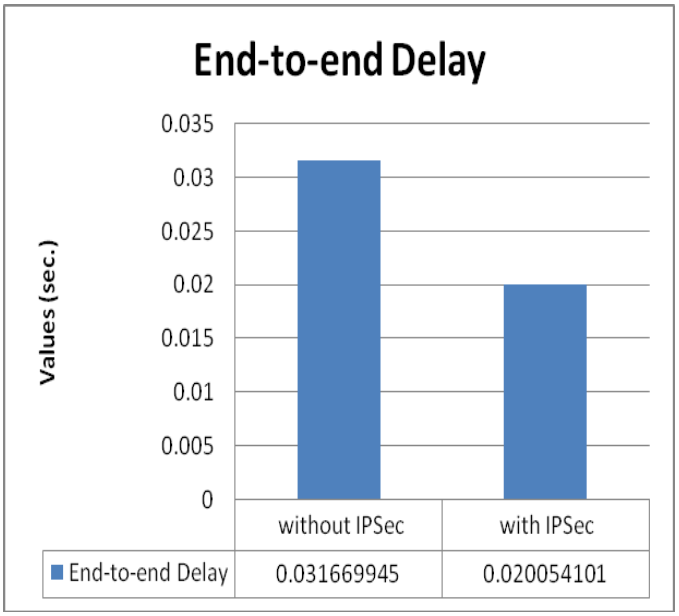

Figure 4. End-to-end Delay

The above graph shows the value of end-to-end delay in WSNs. Average end-to-end delay of the data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. The value of end-to-end delay is 0.031669945 sec. Under black-hole attack and when IPSec security is implemented on wireless sensor network then its value decreases to 0.020054101 sec. as shown in figure 4.

C. Jitter (sec.):

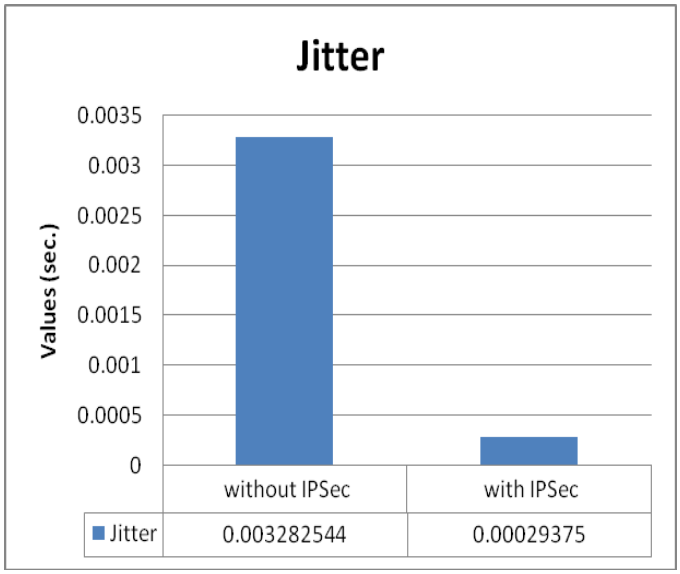

Figure 5. Jitter

The above graph shows the value of jitter in WSNs. The value of jitter is 0.003282544 sec. Under black-hole attack and when IPSec security is implemented on WSN to defend the network against black-hole attack then the value decreases to 0.00029375 sec. as shown in figure 5. The network is considered to be efficient and reliable if its jitter as well as the packet drop ratio is less.

D. Total packet received:

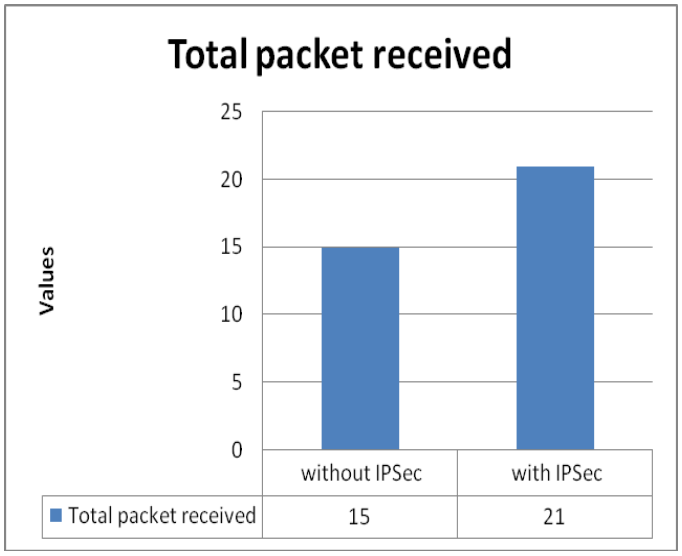

Figure 6. Total packet received

The above 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 black-hole attack is encountered

© 2010, IJARCS All Rights Reserved

on WSN are 15 out of 48 as shown in figure 6 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 21 as shown in graph 6.4. The packet loss rate is less when IPSec is applied to wireless sensor network as compared to under attack.

VII. CONCLUSION

In this paper, we present an approach to prevent the black-hole attack with IPSec protocol in wireless sensor network and the result is evaluated on the basis of metrics like throughput, end-to-end delay, total packet received and jitter. The IPSec scheme is based on symmetric key cryptography based schemes and it is considers as the main source of security in Wireless Sensor Network, till date. The selection of the appropriate cryptographic scheme depends on the processing capability of the sensor nodes characterized by the limited constraints such as its energy, computation capability, bounded memory and communication bandwidth. The mobility of sensor nodes has a great influence on sensor network topology. It is concluded that the throughput of WSN is increased when cryptographic technique is applied to defend against black-hole attack. 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 jitter is less and total packet received is increased in the network when IPSec is implied on it. The IPSec protocol efficiently prevents the black hole attack in WSN.

VIII.REFERENCES

[1]. W. Znaidi, M. Minier and J. P. Babau, "An Ontology for Attacks in Wireless Sensor Networks" Institute National De Recherche En Informatique Et En Automatique (Inria), Oct 2008.

[2]. M. Saxena, "Security in Wireless Sensor Networks: A Layer-based Classification", Department of Computer Science, Purdue University.

[3]. Z. Li and G. Gong, "A Survey on Security in Wireless Sensor Networks", Department of Electrical and Computer Engineering, University of Waterloo, Canada.

[4]. A. Dimitrievski, V. Pejovska and D. Davcev, "Security Issues and Approaches in WSN", Department of computer science, Faculty of Electrical Engineering and Information Technology, Skopje, Republic of Macedonia.

[5]. J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey", Elsevier's Computer Networks Journal 52 (2292-2330), Department of Computer Science, University of California, 2008.

[6]. G. padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security (IJCSIS), vol. 4, No. 1& 2, Department of Computer Science, Avinashilingam University for Women, Coimbatore, India; 2009.

[7]. T. A. Zia, "A Security Framework for Wireless Sensor Networks", Doctor of Philosophy Thesis, The School of Information Technologies, University of Sydney, Feb 2008.

[8]. T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security, 2009.

[9]. A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", In Communications of the ACM Vol. 47, No. 6, 2004.

[10]. Y. Zhou, Y. Fang and Y. Zhang, "Security Wireless Sensor Networks: A Survey", IEEE Communication Surveys, 2008.

[11]. Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In 1st IEEE International Workshop SNPA'03, May 2003.

[12]. Anthony D. Wood and John A. Stankovic. Denial of service in sensor networks. IEEE Computer, 35(issue 10): 48–56, Oct 2002.

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

[14]. 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.

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

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

[17]. 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.

[18]. 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.

[19]. Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M., "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent", International Conference on Artificial Intelligence and Embedded Systems, Singapore, 2012, pp. 45- 48.

[20]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, " Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[21]. Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad, "The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures" International Journal of Wireless and Microwave Technologies, 2012, Vol. 2, pp. 33-44.

[22]. Nadeem Ahmed, Salil S. Kanhere and Sanjay Jha, "The Holes Problem in Wireless Sensor Networks: A Survey", Mobile Computing and Communications Review, Volume 1, Number 2, pp. 1- 14.

[23]. Chris Karlof and David Wagner, " Secure routing in wireless sensor networks: attacks and countermeasures", Elsevier-joutnal of Ad-hoc networks, 2003, pp. 293- 315.

© 2010, IJARCS All Rights Reserved