Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CONCEPTION OF THROUGHPUT BY PREVENTING FLOOD ATTACK IN NETWORK LAYER

[1]C.DHIVYA DEVI,[2] G.NANTHA KUMAR,[3] DR. A.AROKIASAMY

[1]Assistant Professor, Department of CSE, Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tamil Nadu, India.
[2] Research Scholar, Anna University, Chennai.
[3] Professor, Department of CSE, E.G.S.Pillay Engineering College, Nagapattinam, Tamil Nadu, India.
E-mail: [1]divyamtech89@gmail.com, [2]gan_nand@yahoo.com, [3]a.arokiasamy@gmail.com

ABSTRACT

To achieve the target potential in wireless sensor networks, security has been creating a major role where it has been used during the communication of nodes in a specified area, by considering the secure connections between the nodes during the transmission of packets. As per security as concern, wireless sensor networks has been deployed in several environments, where providing a genuine barrier for the malicious nodes in the specified area is a major challenging task. While there are many disputes, in this article we primarily focus on security of wireless sensor networks by creating and establishing the impact of attacker nodes in the simulated area by using aodv protocol which has been modified by giving values for the creation of malicious nodes through Black hole AODV. Further, we propose the simulated area of network to attain the level of security by introducing key generation technique and intrusion detection system to keep track of monitoring the throughput evaluation which is being calculated by varying the number of each and every connection by fixing the number of attackers constant throughout the network simulated area.

Key words: *Hello Flood Attack, Attackers, Ad-Hoc Routing, Security, Authentication, Intrusion Detection System, Throughput.*

1. INTRODUCTION TO WIRELESS SENSOR NETWORKS:

The extremely undefendable to attacks which is being framed with plenty of small and micro sensory devices with less energy, memory and power is the existence of wireless sensor network. The area covered by WSN application has raised the level of security to the adoption and consumption of sensor networks without any interrupts throughout the wide area of occurrence. Sensor networks are interacting with very sensitive data and deployed in hostile unattended environments, where the security issues should be concentrated to attain their potential.

WSN is a substantive part of the network, popped out with a smatter application such as medical applications, environmental pollution detection, agribusiness etc., even there is a presence of confinements over characteristics like battery power, low energy consumption which calls for a lot of care to keep off network's life time reduction profiting from security problems consumed on WSN. To meet the better performance in WSN, it is a mandate thing to provide a good path.

To demonstrate the data flooding attack, an illegal node create a route to the prey node and starts sending an enormous incorrect data packets to the prey node through that route. Because of this action, definitely the attack will bring down the functioning level of the network to an unexpected situation. Here the security issues should be considered over a given network for the creation of goodly environment in wireless sensor networks.

2. RELATED WORK AND OUR CONTRIBUTIONS

The perspective view and analysis of flood attack by different authors in different papers have been listed in the TABLE 1 with the brief descriptions as follows.

Table 1: Analysis of Methods

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Analysis of Methods

S.No	Author name	Method
1.	Revathi et al.:[13]	Extended DSR is implemented in ad hoc network.
2.	Virendra Pal singh et al:[9]	Detection of hello flood attack on signal strength and client puzzle method.
3.	Mohamed M.Ibrahim et al:[11]	REHIDAN algorithm to identify flooding attacker nodes.
4.	H.Kim et al.:[7]	PDM novel Period based Defense Mechanism.
5.	Vuanyuan Zhang and Wassim Znaidi [6]	Multi path ACK scheme

DESCRIPTIONS:

The brief descriptions for the methods listed on above table.

***Method 1*:**

Dynamic Source Routing uses source routing at each intermediary nodes on behalf of previous routing tables. In[13], the author have considered the neighbouring nodes as strangers, acquaintances and friends with different threshold values by implementing the algorithm in both RREQ flooding attack and DATA flooding attack using the extended DSR protocol.

The following Fig.1. shows the performance analysis(evaluation) of throughput by varying the parameters such as exceeding malicious nodes, number of connections and mobile nodes of connections, excluding the measurement of time, using extended DSR rather than regular DSR.

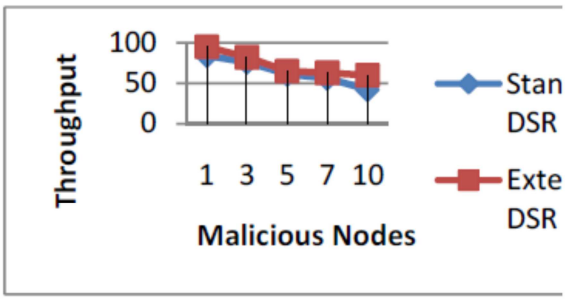

Fig.1. *Malicious Nodes vs Throughput*

***Method 2*:**

The authors have considered some primary assumption such as all sensor nodes are homogeneous, communicating within a fixed radio range which knows the fixed signal strength along with a time threshold, to detect the hello flood attack which is grounded on signal strength and client puzzles method in [9]. He uses the two ray propagation model to calculate the strength of signals.

Possibility of receiving hello message at each node which, have the signal strength equal to that of fixed strength, then it comes under stranger or a friend. Short client puzzles which is in a fond of less computational and battery power is highly suitable to verify the validity of valid nodes. The difficulty of puzzles can be made using Dynamic policy technique allotted to the strangers based on the number of hello messages sent.

***Method 3*:**

The Ad hoc On - Demand Distance Vector Routing protocol which have a chance to forward the control and data packets in randomized dynamic topology of connection, but it could not address all the possible attacks. To overcome the above problem, the Real-time Host Intrusion Detection for Ad hoc Networks (REHIDAN) algorithm is used [11], to minimize the effectiveness of the attacks. Intrusion detection approach having the functions like Monitoring, analysing, assessing, recognizing, and tracking are examined by author. The REHIDAN algorithm in [11], uses the idea of neighbour suppression algorithm isolating through which, the attacker is isolated from the neighbour nodes. It is implemented, with OPNET.

***Method 4*:**

The main concept of Period based Defense Mechanism (PDM) in [7], is flooding of data attack, by which the attacking nodes by it make them believe the other nodes of connection and will able to send most vulnerable data packets over the path of a connection. Most probably on the other side to bring down the level of defense over a flooding attack, the blocking path way should be taken over where, the major traffic from other traffic of attacks.

***Method 5*:**

Process of finding the optimistic solutions of information that binds on the network in order to pointed out both the data

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

flows and acknowledgement flows.

Because of being under the multipath possibility of the simulated area of connection, which could have been blocked over to an attack of selective forwarding attacker nodes, which might have a chance for occurring of dropping of packets all around the simulated area of connections. Multi-hop multi-stream unicast routing protocol, gradient based routing protocol are used for implementation.

Method 6:

Through identity verification protocol, hello flood attack has been counter balanced which further checks the bi-direction link of nodes deployed in an area. The method was being useless if the enemy nodes has been with high range of transmitting powers over an simulated area. This might have not will have chance to detect or control the flooding of hello messages around the connections.

Method 7:

Solution framework has been implemented in [17] where the author has used that to avoid the sequence of actions against the denial of service attack. The puzzles have been established to keep on protection from various attacks which allow the all nodes to solve the puzzles.

The importance of punishing attacker's nodes will keep on increasing the difficulty of puzzles by increasing the burden for the other valid nodes also.

Method 8

The author has proposed the security mechanism for the nodes in the simulated area by taking the signals as an input for their modules which will have a chance to detect the attackers around the area of network which having the attack of hello flood.

Method 9

The importance of handshake protocol has been implemented for a network area by keep on connecting the valid nodes with the attackers by performing request and reply from the source to the destination on the basis of neighbours its gets connected. This may have a chance to affect the valid nodes by changing their presence in a valid condition.

The collision will occur between the nodes which was under the range of high density during the time of arrival which will further decoded and they night have a chance to hear the replies of victims.

Method 10

To check whether the mobile node neighbours are intruders or not, the authors decided to use the threshold values for the mobile nodes proposed in [20] the sequence of an order should be followed in name of dispute over attacker of flooding messages happened in MANET. The possible condition to come to a solution of finding the nodes as intruders is if the node value of routing packets outmatches the given value of threshold range of connections.

3. PROBLEM DEFINITION

The proposed system of architecture implemented on the network simulator ns-2, with distribution of random nodes relied on the network field of size 750 m * 750 m.

The conception of throughput analysis is based on the creation of nodes with the implementation of attacks on it. The nodes created on the simulated areas with the energy model with the initial energy of 100 specified with the receiving and transmitting range of 0.2. The idle time and the sleeping time of nodes can be specified around the simulated area of connections during transmissions.

The AODV protocol has been used here for the transferring of control and data packets around the simulated area by considering the shortest distance of neighbouring nodes within the connections. The normal transferring of packets between the nodes have been implemented using the AODV protocol.

By considering black hole AODV, the protocol is implemented for nodes considered as an attacker to violate the security among the valid nodes. The control packets and data packets are transferred on the basis of shortest path found by the nodes to establish communication with other nodes through the nearest neighbours for the communication. Dropping of packets may occur due to action of attacker over the other valid nodes, by violating the path travelled by the attackers over on other nodes along the distance of neighbours it reaches.

As the communication between the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes goes on, the initial energy range of nodes will reduces as it reaches the path to destination around the area. The reduction of energy can be obtained and monitored using the variation of colours from green to black as the transmissions goes on simultaneously. The violation of attackers on the area is strictly prohibited by implementing the black hole aodv protocol and intrusion detection system has been connected using the RSA authentication technique to detect and avoid the key formation for the invalid nodes called attackers.

By increasing the number of nodes for a given area as fixing the attackers in it will have a chance to make believe that the attackers is also included under the neighbours list. To overcome this issue, the generation of key is handled for a valid nodes by creating an ID and key for a separate nodes of deployment. The nodes which is considered to be an attacker must have any key or ID on its list to make believe other nodes on the range. As the communication goes on by this technique, the attackers will not violate the valid nodes and the dropping of packets will be avoided throughout the connection of transferring packets.

Since the control packets and data packets have been transmitted around the network area, energy reduces over a simulated area from changing the colour from green to black to indicate the energy levels of an each and every node. As the communication goes on, the reliability of a simulated connected area relies on the key management technique of generating a keys and id for valid nodes.

4. DESIGN AND IMPLEMENTATION

Intrusion detection system (IDS) supervisors the nodes which have been deployed in a simulated area through the linkage of nodes together. It is responsible for the avoidance of malicious traffic by performing actions like stopping the source or destination ip address by making them not accessing the network.

The major goal is the effective monitoring sense of connections have been established around the simulated area by keep on tracking the nodes which are creating traffic in the form of attackers.

The RSA consist of three key generation techniques. The authentication is a key barrier in the network information system security field. RSA is a open network environment technology, using public key cryptogram system theory has implemented and supplied a universal security infrastructure for security services, it has two main application, include encryption and digital signature. Along with the modern times autoimmunization improvements, a great deal of no face-to-face electronic trades are increasing.

A veracity, and security, and practicable automatic personal identification are even more highly demanded and required in our life. Developed a suit of simple identity authentication system for encryption and authentication, it supply a base of research and development.

RSA encryption, supplies unique and stability technology advantages, presents a authentication system. Using the public key (PKA) or asymmetric key algorithm, the usage of both public and private key will provide the effective secur connections around the simulated area of deployment.

The sharing of public key is used by the nodes in an area to encrypt and decrypt the data's. Whereas the private key is not shared to other nodes due the concept of secure connections to be implemented in the network area.

Black hole Attack

The attack has been implemented under the concept of AODV attacks by insisting the malicious nodes inside the code of cc file to activate the black hole attack for the simulated area of connection. The attack will be placed on the network which could spoil the connection of nodes during the data transmissions by spoofing them voluntarily to bring some changes around the network. The might have a chance to control the nodes of the simulated connections by making them believe that they are the original neighbours of the connections.

Authentication

The authentication can be fixed using the generation of keys for valid nodes by implementing the RSA technique using the method of assuming the random numbers taken by the nodes in a simulated area. The attackers might not have a key on its own and the chance will not give for them to violate the valid nodes in the simulated network around the range of connections.

Security

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The proposed system of connections will provide a wide range of security around the simulated area by enhancing the secured formation of keys for an individual node by excluding the attackers as when they reach the invalid nodes during the transmission of control and data packets.

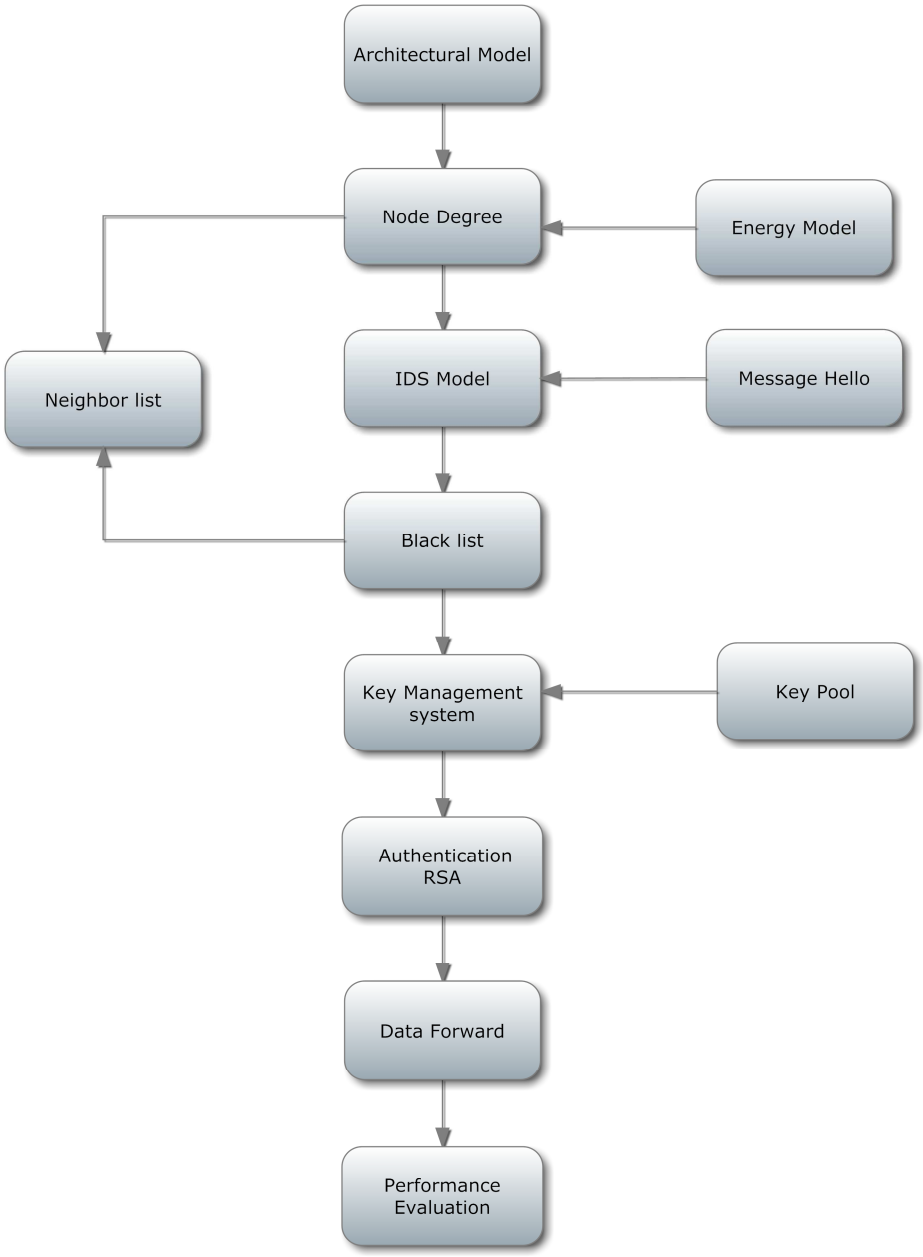

Fig.2. *Flow Diagram for Proposed System*

5. DISCUSSION

Simulated Architectural Model With Attack

The simulation work has been done with The Network Simulator ns-2, Version 2.29. The nodes in the simulated area are randomly distributed within the network field of size 750m * 750m. The network animator shows the simulation results of transferring data's between different deployments of nodes.

Black Hole Attack With Energy Model

The summarization of the black hole attack can be listed with the following bullets,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- The attacker nodes will keep track of following the valid nodes to get the neighbours address.
- The attacker nodes having a chance to send the RREP messages along with receiver address which might have a chance to spoof the unknown receivers whom under the simulated connections.
- The lower value should be given for hop count and the higher value should be given for a sequence number.
- If the attacker nodes finds the path and route to reach the valid node they will definitely send the RREP messages to the valid nodes which belongs to the simulated area of connection.
- The valid nodes will have been sending the replies to the attackers nodes even after it doesn't know about their presence in network area.
- The routing table will be updated by the valid nodes of connections only after the required information can be received.
- The valid nodes will always prefer for a new route of connection for the purpose of data forwarding technique.
- The attacker nodes can easily drop the packets whoever involved in the simulated area of connections by making them believe that they are valid and neighbours of others.

Data Forwarding:

The control packets and data packets are transmitted during the communication involved among the nodes around the simulated network area by considering the path of shortest distance to reach the source and destination, implemented using the method of aodv protocol.

Packets will be in a position to travel along the shortest path to reach the nearest neighbours executed using the aodv protocol as it is being a reactive protocol and it will establish a perfect route to the destination nodes only based on the demand of connection. In aodv, the source node and an intermediate node will maintain the information about the next hop information.

Random Key Generation Using Rsa Authentication

In our proposed we use RSA based key generation. And then we use of hashing technique for memory optimization. We create one pair wise key and one shared key.

RSA encryption, supplies unique and stability technology advantages, presents a authentication system. Using the public key (PKA) or asymmetric key algorithm, the usage of both public and private key will provide the effective secure connections around the simulated area of deployment.

The black hole attack is a kind of denial of service attack where it will disrupt the network and the result affects the whole performance of the network. The attack is made by malicious node which attacks the AODV control message.

The sharing of public key is used by the nodes in an area to encrypt and decrypt the data's. Whereas the private key is not shared to other nodes due the concept of secure connections to be implemented in the network area.

The method of implementing the generation of new keys to the nodes especially to the valid nodes by excluding the attackers from the simulated area of connections will improve secure connections between all different deployed nodes.

The valid nodes will not have a chance to communicate with the nodes in the form of attackers in which the secure communication and transmission of data can be established.

Prevention Of Attack Using Intrusion Detection System

To prove our model we need to formulate an adversary model in our network. Adversaries are intruders in our network they do false things against the protocol. The adversary model here for monitoring the network activities such as record data, time and size of the packet

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

sent over the network also it observes the source and destination nodes id for disrupting the packet transmission.

Intrusion detection system (IDS) supervisors the nodes which have been deployed in the simulated area with help of linkage of nodes together. It is responsible for the avoidance of malicious traffic by performing actions like stopping the source or destination ip address by making them not accessing the network.

The major goal is the effective monitoring sense of connections have been established around the simulated area by keep on tracking the nodes which are creating traffic in the form of attackers.

Intrusion detection system plays a vital role in finding and detecting the types of attackers at a high range of connection. This will surely compares and controls the nodes of both the attackers and the valid nodes to possibly identifying the security issues.

The following bullets insist the capabilities of an Intrusion Detection System,

- Examining and supervising the nodes actions.
- Inspecting the configure manners of all the systems
- Integrated parts of the system and the content files will be checked.
- Comparison of existing attacks with the newly developed attacks in the form of pattern matching.
- Analysing the unnatural contents of the nodes actions.
- Scrutinize the operating system configurations.

Advantages of IDS

the following bullets will provide the usage of IDS system,

- Appending the high integration to system of nodes in connections.
- Tracking the actions of user nodes from the beginning point.
- Indicate if there are any alterations in user contents.
- Keep track of updating the information for various new attacks.
- System which has been attacked with attacker can be detected.
- Errors in the configuration system will be monitored.
- Protect the valid nodes from the attack of malicious nodes.An IDS system will have been tracking on the network by keep tracking on the routes and the connections it involves. The IDS can compare the received information along with the data in the database in the form detecting the misuse of any attacker nodes.

The comparison of control packets and data packets will be taken place with the database information of the nodes connected around the system of connections.

In the case of anomaly detection, the parameters like, network capacity, load and other features has been already fixed by an admin who could able to compare the contents of data in the database. It will monitor the actions of nodes in the simulated area connections around the network.

Routing Table Details

The file is created on the code to display the routing details of source and destination which relies on the request and the reply messages that are transmitted between them at a given range of simulated area.

The contents in routing table file will have collected information about hop count, next hop, flags, source id, and destination id along with current time of transmission in the given range of simulated area.

6. PERFORMANCE EVALUATION

Let us focus on the conception of throughput analysis using the proposed system of architecture implemented with aodv and black hole aodv protocol. The performance evaluation of throughput is predicted by calculating between different number of nodes corresponding to the fixed number of attackers placed on the simulated area.

The gnuplot is a two dimensional graph method to display the graph in a perspective of order to the user defined values.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We will analyze the conception of throughput by plotting graph between throughput values over changing the different number of nodes by keeping the attackers same for all communications with the help of gnu plot.

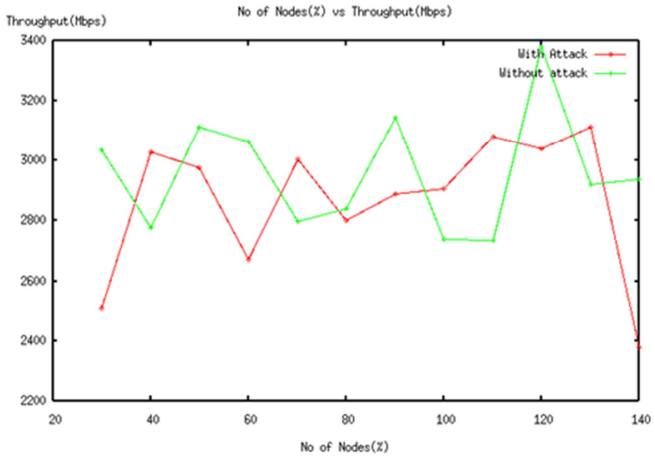

Fig.3. Graph between Nodes vs Throughput in GNUPLOT

Table 2: Table illustrates the values between different nodes and attackers

No.of nodes	With Attack	Without Attack
30	2508	3036
40	3029	2777
50	2978	3113
60	2672	3065
70	3003	2840
80	2803	2840
90	2888	3145
100	2908	2738
110	3082	2736
120	3038	3380
130	3113	2919
140	2376	2937

7. CONCLUSION AND FUTURE WORK

In our paper, we have presented a new approach for secure data transferring between nodes against various malicious nodes. Intrusion detection system has been implemented to detect the malicious nodes in the given area with the AODV protocol by creating a BlackHoleAODV protocol. The Random key generation technique provides authentication by generating keys for valid nodes alone which prevents the valid nodes from the attack of malicious nodes by increasing the throughput performance as a measure.

Our future is based on the mobility of the nodes along with the time measure to exclude the adversary from the network through the identification of the malicious nodes via signal strength comparison.

REFERENCES

[1] Jalil Jabari Lotf, Seyed Hossein Hosseininazhad Ghazani, "Security and Common Attacks Against Network Layer In Wireless Sensor Networks", J. Basic. Appl. Sci. Res., 2(2) pp. 1926-1932, 2012.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[2] Dimple Juneja, Atul Sharma, and A.K. Sharma," Wireless Sensor Network Security Researchand Challenges: A Backdrop", HPAGC, CCIS 169, pp. 406–416, 2011.
[3] S.H. Jokhio, I.A. Jokhio, and A.H. Kemp," Node Capture Attack Detection And Defence In Wireless Sensor Networks", IET Wirel. Sens. Syst , Vol. 2, Iss. 3, pp. 161–169 2012.
[4] Saurabh Singh, Dr. Harsh Kumar Verma ,"Security For Wireless Sensor Network ", International Journal On Computer Science And Engineering (IJCSE) Vol. 3 No. 6 pp. 2303-2399 June 2011.
[5] Suraj Sharma And Sanjay Kumar Jena," A Survey On Secure Hierarchical Routing Protocols In Wireless Sensor Networks", ICCCS'11 February 12-14, pp. 146-151, Rourkela, Odisha, India, ACM 2011.
[6] Yuanyuan Zhang, Wassim Znaidi, C´Edric Lauradoux And Marine Minier," Flooding Attacks Against Network Coding And Countermeasures ", pp. 305-309, IEEE 2011.
[7] Hyojin Kim, Ramachandra Bhargav Chitti, And Jooseok Song," Novel Defense Mechanism Against Data Flooding Attacks In Wireless Ad Hoc Networks", IEEE Transactions On Consumer Electronics, Vol. 56, No. 2, pp. 579-582 May 2010.
[8] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview On Its Security Threats," IJCA Special Issue On "Mobile Ad-Hoc Networks"Manets, pp. 42-45, 2010.
[9] Virendra Pal Singh, Sweta Jain And Jyoti Singhai, "Hello Flood Attack And Its Countermeasures In Wireless Sensor Networks", IJCSI International Journal Of Computer Science Issues, Vol. 7, Issue 3, No 11, pp. 23-27, May 2010.
[10] Hemanta Kumar Kalita And Avijit Kar," Wireless Sensor Network Security Analysis", International Journal Of Next-Generation Networks (IJNGN), Vol.1, No.1, pp. 1-10, December 2009.
[11] Mohamed M. Ibrahim, Nayera Sadek, Mohamed EI-Banna "Prevention Of Flooding Attack In Wireless Adhoc AODV-Based Networks Using Real-Time Host Intrusion Detection" pp. 1-5 IEEE 2009.
[12] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey Of Attacks, Security Mechanisms And Challenges In Wireless Sensor Networks", (IJCSIS) International Journal Of Computer Science And Information Security,Vol. 4, No. 1 & 2, 2009.
[13] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka, T. Rama Rao," Prevention Of Flooding Attacks In Mobile Ad Hoc Networks", International Conference On Advances In Computing, Communication And Control (ICAC3) pp. 525-529, 2009.
[14] Xiangqian Chen, Kia Makki, Kang Yen, And Niki Pissinou, " Sensor Network Security: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER pp. 52-57, 2009.
[15] Xiaojiang Du And Yang Xiao," A Survey On Sensor Network Security" pp. 403-421, 2007.
[16] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, " A SURVEY OF ATTACKS AND COUNTERMEASURES IN MOBILE AD HOC NETWORKS" , In Wireless Network Security, pp.103-135, 2007.
[17] Zhen Cao, Xia Zhou, Maoxing Xu, Zhong Chen, Jianbin Hu, Liyong Tang , (2006), Enhancing Base Station Securityagainst DoS Attacks in Wireless Sensor Networks, IEEE.
[18] Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, (2004), Malicious Node Detection in Wireless Sensor Networks, IEEE.
[19] Mohammad Sayad Haghighi , Kamal Mohamedpour, (2008), Securing Wireless Sensor Networks against BroadcastAttacks, IEEE.
[20] Bo-Cang Peng, Chiu-Kuo Liang, (2006), Prevention Techniques for Flooding Attacks in Ad Hoc Networks, IEEE.
[21] Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.
[22] A Hamid, S Hong, (2006) Defense against Lap-top ClassAttacker in Wireless Sensor Network, ICACT.