P-ISSN: 2347-4408
E-ISSN: 2347-4734

IDC BASED PROTOCOL IN AD HOC NETWORKS FOR SECURITY TRANSACTIONS

[1]K.Priyanka [2]M.Saravanakumar
[1]Student M.E.CSE,
[2]Asst. professor, Department of CSE,
Maharaja Prithvi Engineering College, Avinashi.
[1]k.priyankha@gmail.com

Abstract— Paper describes a Self-configured, Self organizing protocol that encompasses IDC (Identity Card) – unique identity to provide security and trust in spontaneous wireless ad hoc networks. IDC is generated and encrypted as signatures and gotten certificate for trust with a Distributed Certification Authority. A trusted node exchanges IDC and ensures Authentication. Data services can be offered to the authenticated neighboring nodes without any infrastructure and saves time. Services can be discovered using Web Services Description Language (WSDL). Untrustworthy nodes enroll with Intruded Signatures and (DANIDS) Intrusion Detection System blocks affected node and alert all other nodes in network.

Keywords— Identity Card Security, Distributed Authority, Signatures, Authentication, Intrusion Detection System,

1. INTRODUCTION

MANET (Mobile Ad hoc Network) refers to a multi hop packet based wireless network entangled with a set of mobile nodes that can communicate spontaneously. The design of a protocol allows the creation and management of a spontaneous wireless ad hoc network with highly secured transactions and with little human intervention. No Infrastructure is required and is intended to self organize based upon the environments and availability. Security, Trust and Authentication is the key feature included. Network is self configured based up on the physical and logical parameters provided and network begins with the first node and is widespread by attaching forth coming nodes as neighbor nodes in the network, thereby achieves scalability. Protocol encloses IDC (Identity Card) having two components public and private to provide security and trust in networks. Encrypted form of IDC evaluates Digital Signatures and is certified and trusted. No Centralized Certificate Authority is included. Joining Node with configured network and Communication between the nodes is done only based on trust and certificate issued by the Distributed Certificate Authority. A trusted node exchanges their IDC with each other and ensures Authentication. Thus reliable and secure communication is enabled. Data services can be offered to the authenticated neighboring nodes without any infrastructure and saves time. Various paths to reach destination could be determined by nodes itself. Services can be discovered using Web Services Description Language (WSDL). A node receives a data packet that is ciphered by a public key. When the server process received the packet, it is in charge of deciphering it with the private key of the user. When the data is not delivered properly, it is not acknowledged and retransmission is done by the user. Untrustworthy nodes are blocked by Intrusion Detection Mechanism within the protocol.

1.1 MANET

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

Working of MANET

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics. Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANET are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructure (e.g., a mixture of fixed and mobile routers) is supported.

Characteristics of MANET

In MANET, each node acts as both host and router. It is autonomous in behavior. The nodes can join or leave the network anytime, making the network topology dynamic in nature. Mobile nodes are characterized with less memory, power and light weight features. Mobile and spontaneous behavior demands minimum human intervention to configure the network. All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment. High user density and large level of user mobility is present. Nodal connectivity is intermittent.

Forms of Connections

Infrastructure-based Networks

It is form of network without any access point. Every station is a simultaneously router that includes the authority control to be centralized. Nodes communicate with access point and are suitable for areas where AP is provided. Figure 1 depicts this form of network.

Infrastructure-less Networks

It is form of network without any backbone and access point. Every station is a simultaneous router that includes the authority control to be distributed. Figure 2 depicts that network is formed with no backbone and access point. Any node can access any other node without centralized control.

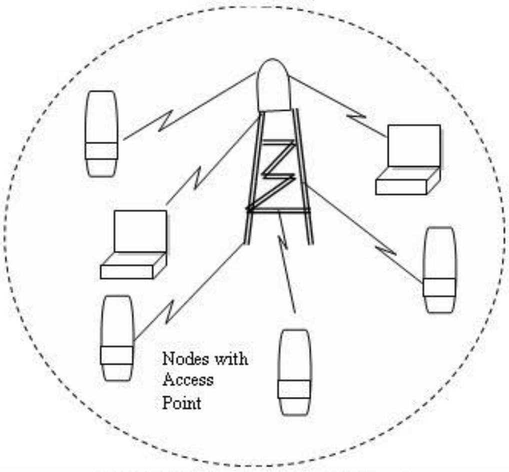

Fig 1 Infrastructure based Networks

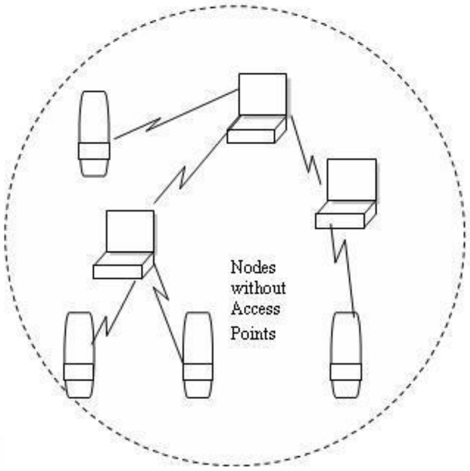

Fig 2 Infrastructure less Networks

2. Implementing IDC Security in Protocol

The protocol proposed in this paper can establish a secure self-configured Ad Hoc environment for data distribution among users. Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority between the users that trust the new user. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification.

Advantages

The basis is to setup a secure spontaneous network and solve several security issues. Authentication phase is included based on IDC (Identity Card) that helps in unique identification of node. Each node is identified uniquely with a public key and LID after authentication process that verifies the integrity of the data. Trust phase includes each and every trusted node to behave as distributed authority and to have direct communication without any central control. Validation of integrity and authentication is done automatically in each node. There exists a mechanism to allow nodes to check the authenticity of their IP addresses while not generating duplicated IP addresses. The mechanism helps nodes to authenticate by using their IP addresses. It does not require any infrastructure and every node self configure the logical and physical parameters automatically without any user intervention. Flooding of the data to all nodes in the network is avoided by allowing each individual node to choose a path to reach the destination. Hacking signatures - a class of Intrusion Detection can be blocked and prevented. Also Intrusion can be alerted to all individual users in the network. This is shown in fig.3.

2.1 Registration

User accesses application and provides Identity Card information to the system protocol. New Node and Network are created. Node Join Approach (Distributed Algorithm) authenticates the information to join the node in the network. Services are discovered. Data is Delivered and acknowledged. Hacked nodes are detected and blocked with an alert. IDC include Public Component comprises of Logical Identity- unique ID, public key and an IP. Private Component of IDC includes private key.

2.2 Node Creation

The basic idea behind is to encrypt the registered IDC information along with encrypted message. IDC generates Message Digest generated by SHA Algorithm. It is encrypted with user’s public key known to be Digital Signature. Each of the nodes is validated with Distributed Certificate Authority and is considered to be trusted node and thus provides Node Creation. Public key, LID and Private Key is assigned and is given for data exchange. If failed the device won’t exchange data. The User introduces its personal data while login at first time and the security information is generated. Data are stored persistently in the device. Both clients and servers can request or serve requests for information or authentication from other nodes. User Certificate has expiration.

SHA-1 Algorithm

SHA-1 algorithm uses 160 bit. A Hash value is generated by a function H of the form h=H (M), where M-variable length message and H (M)-fixed length hash value. It takes as input a message with maximum length of less than 2^{64} bits and produces output a 160 bit message digest. The Input is processed on 512 bit blocks. Word Size includes 32 bits and number of step includes 80. Process includes, Appending padding bits and length, Initialize MD Buffer, Process message in 512 bit blocks, and Producing Output.

In this module, we create a new network for the trusted users. Network is created by Logical and Physical configuration parameters that are passed and each node generate the session key that will be exchanged with new nodes after authentication. Each node configures its own data including the first node. The data include IP, port, user data and data security. Network begins with the first node and is widespread by attaching forth coming nodes as neighbour nodes in the network without restrictions, thereby achieves scalability. Nodes can also send requests to update network information. Reply will contain identity cards of all nodes in the network. Nodes replying to the request must sign this data ensuring authenticity. The owner provides session key. The data is shared between two trusted users by session key for their respective data's and encrypting their files.

Network Configuration Module

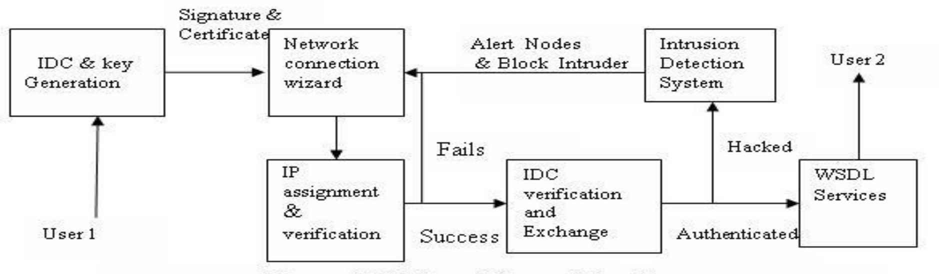
Signature & Certificate
IDC & key Generation
Network connection wizard
Alert Nodes & Block Intruder
Intrusion Detection System
User 2
Fails
Hacked
IP assignment & verification
IDC verification and Exchange
WSDL Services
User 1
Success
Authenticated

Figure 3 IDC based Protocol Architecture

AES Algorithm

Session key is generated by AES (ADVANCE ENRYPTION STANDARD) Algorithm. Symmetric Key is used as Session Key to cipher the confidential message between trusted nodes and uses 128 bit key length and block length. Number of rounds is 10. Round Key Size is 128 bits and expanded key size is 176 bits. It offers high security because its design structure removes sub key symmetry. Also execution time and energy consumption are adequate for low power devices. The user can only access the data file with the encrypted key if the user has the privilege to access the file. Encryption process includes Add round key, Substitute bytes, Shift rows and Mix columns. Decryption involves inverse sub bytes, Inverse shift rows, Inverse mix columns and Add round key. Session key has an expiration time, so it is revoked periodically. All these values are stored in each node.

2.3 Node Joining

It employs a distributed algorithm called Node Join approach. Joining the node in network is done only if attain trust and gotten certificate from a valid Distributed CA. Next, Trusted nodes exchange IDC and Authentication is done using IDC (Identity Card) and the Certificate. Also Node authenticates a requesting node by validating the received information, by verifying the non duplication of the LID and IDC. IP assignment is done further if authentication got success. If Authentication fails, determines intrusions in the network. WSDL (Web Services Description Language) configures network and delivers the data and acknowledges if delivered to the destination. When the node is authenticated it is able to perform operations either transparently or by individual user. The authenticated node can display the nodes, send data to all nodes, join and leave the network. After authentication, they are provided with IDC (Identity card and Certificate) for further communication. There are only two trust levels in the system. Any 2 nodes can trust each other or can be trusted mutual neighbour node.

RSA Algorithm

The Asymmetric key encryption schemes RSA is used for Distribution of Session key and Authentication process. RSA includes 512-bit key and 1024 bit. RSA scheme is a block cipher in which plain text (M) and cipher text (C) are integers between 0 and n-1 for some n. Typical Size includes 1024 bits. Plain text is encrypted in blocks, with each block having a binary value less than or equal to $\log_2$ n. Block Size is 'k' bits. Both sender and receiver must know the value of n. Sender knows value of e and only receiver knows value of d.

2.4 Data Transfer

Services can be discovered using Web Services Description Language (WSDL) if a node asks for the available services. Services include Data Packet Delivery to any of the trusted nodes. Node will forward the packet to its neighbours. Any path to reach destination can be determined by the user. Flooding of information to all nodes is avoided. This is helpful, when the neighbour is an intruder and is blocked. At that time, user can choose another path to reach destination. This saves times. When the data is properly delivered to the trusted nodes, acknowledgement is given by sender. When the data is not delivered properly, it is not acknowledged or the time expires, retransmission is done by the user. A node receives a data packet that is ciphered by a public key. When the server process received the packet, it is in charge of deciphering it with the private key of the user. To send the encrypted data with the public key to a node, user selects remote node and write the data. Message is encrypted using remote node's public key. Application encrypts the data with the public key, generates the packet and sends it to the selected node.

3. Intrusion Detection

Intruder –Thrust one and producing a sudden onslaught making the system deteriorate or blocked. Systems possessing information on abnormal, unsafe behaviour (attack) is often detected using various intrusion detection systems. The channel is shared, and due to lack of centralized control, the nodes in the network are vulnerable to various attacks from the intruders.

3.1 DANIDS Architecture

The Distributed Agent Network Intrusion Detection System, (DANIDS) is a collection of autonomous agents running within distributed systems, detects Intrusions. It is proposed a response based intrusion detection system which uses several mobile IDS agents for detecting different malicious activities in a node. These multiple IDS agents detect and locate the malicious nodes. The proposed systems rely on the data obtained from its local neighbourhood. Thus, each node possesses signatures (data from neighbour) found in logs or input data streams and detect attack. Log is known to be audit trail data. Signature analysis is based on the attacking knowledge. They transform the semantic description of an attack into the appropriate audit -trail format depicted in fig 4. Each audit trail record contains the following fields: *Subject*: Initiators of actions. A subject is typically a node user or process acting on behalf of users or groups of users. Subject issuing commands constitute entire activities and may be different access classes that may overlap. *Action*: Operation performed by the subject on or with an object; for example, login, read, perform I/O, execute. *Object*: Receptors of actions. Examples include files, programs, messages, and records. Object granularity may vary by object type and by environment. *Exception-Condition:* Denotes which, if any, exception condition is raised on return. *Resource-Usage:* A list of quantitative elements in which each element gives the amount used of some resource (e.g. number of records read or written, session elapsed time). Time-Stamp: Unique time-and-date stamp identifying when the action took place. From this data it constructs the information about the entire network. Each Agent continuously overhears the neighbour nodes activities and records in audit trail. The node prepares the control data embedded in each packet that helps to identify the malicious nodes. The neighbour node utilizes this data and updates it further to detect the malicious nodes. On detection, all other nodes are sent multiple ALERTS about its malicious activities. Figure 4 shows the overall architecture, which consists of 2 main components,

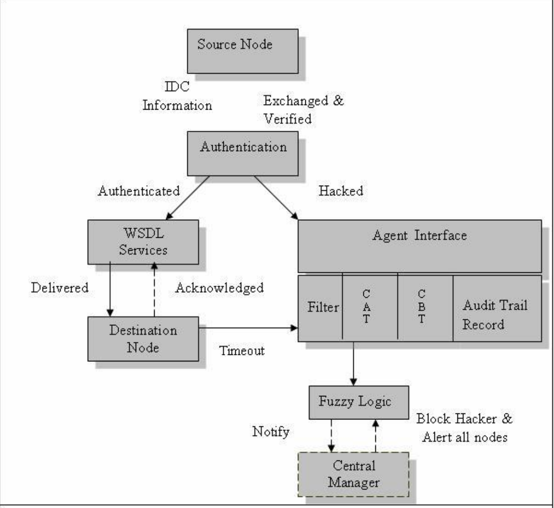

Figure 4 DANIDS Architecture

Agent module: An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security related events on the host and transmit these to the central manager. Each agent can be configured to the operating environment in which it runs. It filters the needed details from the Audit Trail Record and ensures with the fuzzy logic determined.

Central manager module: Receives reports from agents and processes and correlates these reports to detect intrusion. In addition, other third party tools -- LAN monitors, expert systems, intruder recognition and accountability, and intruder tracing tools -- can be "plugged in" to augment the basic host-monitoring infrastructure. The Manager communicates with each agent relaying alert messages when an attack is detected by agent in audit log. We designed Simple Fuzzy rules to identify the misbehaviour nodes.

Filters: The Medium Access Control layer plays an important role in DANIDS. Address registration process guarantee the node's IP address uniqueness. Three new data structures are created at the edge routers: the filtering database, the Internet client's address table, and the Internet client blacklist table. Information extracted from the new ARO and DAR messages are used to fill the filtering database and filtered. It is filled based on the data received from other nodes, client request rate.

Datastructure

The Client Address Table (CAT) includes the client IP address, Life time, number of times it is added to the black list (counter).The Client Blacklist Table(CBT) addresses all client address that encounter lifetime with 0, same IP address determined at more than 1 node and nodes that does not match the encrypted IDC and signature.

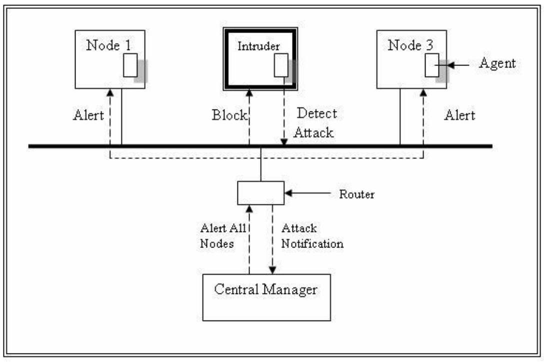

Figure 5 DANIDS Data Flow Diagram

Filtering Packets Received: When the edge router receives/send a packet to a neighbour, agent filters the details and store in audit trail record. It verifies IDC and address of node that matches signatures is filtered to the Client Address Table. Also if its retransmission request it's address if filtered over Client Address Table. Finally if the Signature is not matched or if request node life time expires it is filtered to Black List Table.

Working Procedure

When a node receives a packet from a node it views the audit trail log and decrypts encrypted IDC and signature. It verifies 2 cases, Case 1: If the IDC and signature matches and also verifies black list table to check if IP address is replicated. If it does not match the signature or IP is replicated, Hacked node is detected by the agent and reports central manager. If matches it will communicate and deliver data and acknowledgement is sent. Case2:If the request is for retransmission caused due to time expire of lifetime, it check the client address table for confirmation and resend the data and wait for acknowledgement. In the route-over routing approach, the process is similar as mesh-under approach. 6LRs is used and uses the new DAR and DAC messages to verify the address uniqueness on the edge router. New address registration option (ARO) and duplicate address request (DAR) message formats is included. ARO option contains two fields reserved for future use, the first with 8 bits and the second with 16 bits length. Moreover, the DAR messages also contain an 8 bit length reserved field to implement the security mechanism. Figure 5 depicts this data flow.

Packet Send Ratio (PSR): The ratio of packets that are successfully sent out by a legitimate traffic source compared to the number of packets it intends to send out at the MAC layer. If too many packets are buffered in the MAC layer, the newly arrived packets will be dropped. It is also possible that a packet stays in the MAC layer for too long, resulting in a timeout. If *A* intends to send out *n* messages, but only *m* of them go through, the PSR is m/n. The PSR can be easily measured by a wireless device by keeping track of the number of packets it intends to send and the number of packets that is successfully sent out.

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. *B* may not be able to decode packet sent by A, due to the interference introduced by *X* with an unsuccessful delivery. The PDR may be measured at the receiver that passes the CRC check with respect to the number of packets received. PDR may also be calculated at the sender *A* by having *B* send back an acknowledge packet. In either case, if no packets are received, the PDR is defined to be 0.

3.2 Result Analysis:

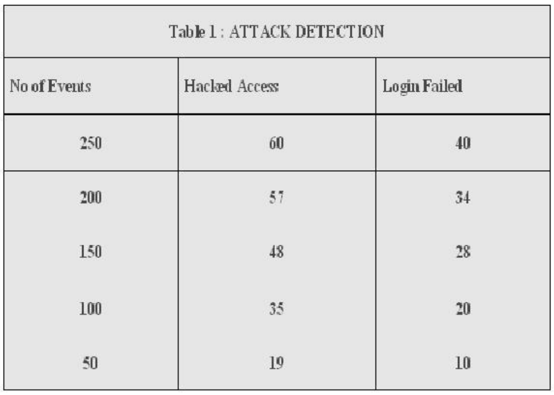

Table 1 : ATTACK DETECTION

No of Events	Hacked Access	Login Failed
250	60	40
200	57	34
150	48	28
100	35	20
50	19	10

Table 1 show that data of audit trail record detecting attacks on MAC Layer and failed login due to time expiry for various number of events given. The graph for the data is presented in figure

6. To detect attack Simple Fuzzy rules are used. The behaviour of the nodes is observed for the past N intervals from a Backup Window (similar to a sliding window). Time Expiration is calculated setting a threshold time interval value of Δ T from small to large. Set as =15 sec, 25 sec and 35 sec and T=1000 millisecond. In Hacked Access, login with wrong password, compared with stored IDC, captured with mismatched IDC and attack detected.

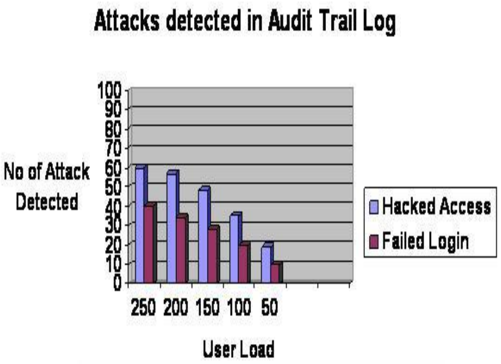

Figure 6 Agent detecting attack from Audit Trail Log

CONCLUSION

In this paper, complete secured protocol implemented in AD Hoc Networks is well defined with little user intervention. No Infrastructure and Central Authority control is required. Each node is identified uniquely with IDC and LID after authentication process that verifies the integrity of the data. Encrypted form of IDC evaluates Digital Signatures and is certified by Distributed Authority. Network is self configured based up on the physical and logical parameters provided and network begins with the first node and is widespread by attaching forth coming nodes as neighbour nodes in the network, thereby achieves scalability. Joining Node with configured network and Communication between the nodes is done only based on trust and authentication. Thus reliable and secure communication is enabled. Data services can be offered to the authenticated neighbouring nodes without flooding and is avoided by allowing each individual node to choose a path to reach the destination. Thereby reduces network traffic and saves times. Services can be discovered using Web Services Description Language (WSDL).Time Expired packets can be retransmitted. Hacking signatures - a class of Intrusion causing Untrustworthy nodes can be detected and blocked by DANIDS (Intrusion Detection System) within the protocol. Also Intrusion can be alerted to all individual users in the network.

REFERENCES

[1] Raquel Lacuesta,Jaime Lloret,Miguel Garcia, Lourdes Penalver,"A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation, IEEE Transactions on Parallel and Distributed Systems Vol.24,No.4, April 2013.

[2] J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless Networks," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 1-8, 2012.

[3] S. Preub and C.H. Cap, "Overview of Spontaneous Networking -Evolving Concepts and Technologies," Rostocker Informatik-Berichte, vol. 24, pp. 113-123, 2000.

[4] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.

[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.

[6] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

[7] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop-by-Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[8] Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005.

[9] Loukas Lazos, and Marwan Krunz, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks" An International Journal on Engineering Science and Technology Arizona edu, Vol.2, No. 2, pp 265-269, April 2010.

[10] R.Vidhya, G. P. Ramesh Kumar, "Securing Data in Ad hoc Networks using Multipath routing", International Journal of Advances in Engineering & Technology, Vol.1, No. 5, pp 337-341, November 2011.