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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

NETWORK INTRUSION DETECTION SYSTEM ON WIRE LESS MOBILE ADHOC NETWORKS

CHILAKALAPUDI MEHER BABU[1], DR. UJWAL A. LANJEWAR[2], CHINTA NAGA MANISHA[3]

M.Tech Scholar, Computer Science & Engg Dept, NIST, VIJAYAWADA (A.P), India[1]

Professor & Research Supervisor, Faculty of Computer Science, R.T.M. Nagpur University, Nagpur[2]

Assistant Professor, Computer Science & Engg Dept, NIST, VIJAYAWADA (A.P), India[3]

Abstract: Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. While developing the sensor nodes in unattended environment increases the chances of various attacks. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper we discussed some attacks on MANET and DDOS also and provide the security against the DDOS attack.

Keywords: Wireless mobile ad-hoc network, security goal, security attacks, defensive mechanisms, challenges, DDoS attack.

1. INTRODUCTION

Network Intrusion detection is the process of monitoring and analyzing events that occur in a computer or networked computer system to detect the behavior of the users that conflict with the intended use of the system. Attacks in MANETs can be classified as Passive attack, Active attack, Network Layer Attack, Transport Layer Attack, Application Layer Attack and Multi Layer Attack. Security for Wireless Mobile Ad-Hoc Networks is becoming an attractive challenge for many researchers. Today's firewalls and encryption software's are not sufficient and effective to protect networks. In Wireless Mobile Ad-hoc Networks there is no centralized control and hence a detection system is needed. The Medium Access Control layer Plays an important role in Wireless mobile Ad-hoc networks. Since the channel is shared, and due to lack of centralized control, the nodes in the network are vulnerable to many attacks from the intruders. The dynamic nature of the Wireless Mobile Ad-hoc networks too demands an intrusion detection system suitable for the MAC layer. Many anomaly based methods are suggested earlier to find an efficient intrusion detection system.

Hence we wanted to propose a response based intrusion detection system for Wireless Mobile Ad-hoc networks 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 neighborhood. From this data it constructs the information about the entire network. Each AGENT continuously overhears the neighbor nodes activities. The node prepares the control data which contain information about how to identify the malicious nodes.

Each mobile node transmits a packet with the control data embedded in it. And the neighbor node uses this data and also updates it further to detect the malicious nodes. The node is not punished in our system; instead the node is sent multiple ALERTS about its malicious activities. And if these reminders reach a certain threshold, the malicious node is simply ignored by the remaining nodes in the network as shown in Fig. 1.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

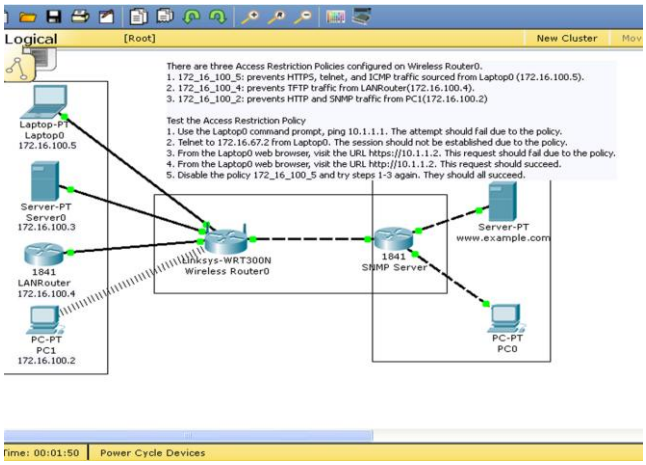


Fig. 1. Example of a simple ad-hoc with connecting nodes.

Our proposed system is suitable for Mobile Ad-hoc Wireless Networks, where it is used to:

1. Detect nodes misbehavior
2. Anomalies in packet forwarding like an Intermediate nodes dropping, Delaying packets.

We designed Simple Fuzzy rules to identify the misbehavior nodes. The main reason for using fuzzy logic in our detection process is that there is no precise difference between a normal and abnormal behavior of a node in the system and also that there are man quantitative features used in every detection systen Generally, the false positive rates are very high i anomaly based detection systems. The behavior of th nodes is observed for the past N intervals from a Backu Window (similar to a sliding window). Any deviatio without proper purpose is reported as an anomaly.

2. INTRUSION DETECTION METHODS AND RELATED WORK.

Intrusion detection systems can be classified broadly int two classes:

- Reputation based schemes.
- Incentive based approaches.

Reputation based schemes detect misbehaving nodes an notify other nodes of the misbehaving nodes. Incentiv based approaches aims to promote positive behavior t foster cooperation instead of relying on participants to report and punish misbehaving nodes. mIDS is a reputation-based system. The authors have detailed intrusion detection methods for the following attacks:

(a) Identifying False route entry in a node's route and
(b) Random packet dropping by intermediate nodes.

The random packet dropping detection scheme relies on overhearing transmissions of neighboring nodes have extended the IDS model described in to enhance the security in AODV (Ad-hoc on demand Distance Vector routing protocol. Watchdog proposes to monitor packet forwarding on top of source routing protocols like DSR. Watchdog has the limitations of relying on overhearing packet transmissions of neighboring nodes for detecting anomalies in packet forwarding. It assumes symmetric bidirectional connectivity: if A can hear B, B can also hear A. Since the whole path is specified, when node A forwards a packet to the next hop B, it knows B's next hop C. It then overhears the channel for B's transmission to C. If it does not hear the transmission after a timeout, a failure threshold associated with B is increased. If the threshold exceeds a maximum value, A sends a report packet to the source notifying B's misbehavior. Reference follows the same concept but works with distance vector protocols such as ADOV. Each node knows about its correct next hop neighbors. It also considers more types of attacks, such as packet modification, packet duplication, and packet- jamming DoS attacks. The proposed a way to detect packet dropping in ad-hoc networks that addresses the Problems of receiver collisions, limited transmission power and directional antennas.

2.1 Detection methods.

Various methods are proposed to detect the intrusion identity. The following are the notations used in such methods Numberof in (m): the number of incoming packets on the monitored node m, as shown in Fig. 2.

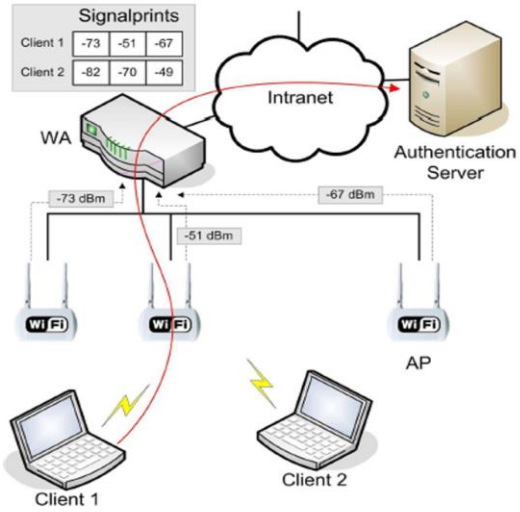


Fig.2. Example of mobility

Applications Number of out (m): the number of outgoing packets from the monitored node m. Numberof_out([m]): the number of outgoing packets of which the monitored node m is the source.

Numberof_in ([m]): the number of incoming packets of which the monitored node m is the destination.

Numberof in ([s]; m): the number of incoming packets on m of which node s is the source.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

Numberofout (m; [d]): the number of outgoing packets from m of which node d is the destination.
Numberofout (m; n): the number of outgoing packets from m of which n is the next hop.
Numberof ([s]; M; m), the number of packets that are originated from s and transmitted from M to m.
Numberof ([s]; M; [m]), the number of packets that are originated from s and transmitted from M to m, of which m is the final destination. Numberof([s];[d]), the number of packets received on the monitored node (m) which is originated from s and destined to d. The detection methods are as follows.

1) Unconditional Packet Dropping

FP (Forward Percentage) FPm = packets actually forwarded → (1) packets to be forwarded FP determines the ratio of forwarded packets over the packets that are transmitted from M to m and that m should forward. If the denominator is not zero and FPi = 0, the attack is detected as Unconditional Packet Dropping and m is identified as the attacker.

2) Random Packet Dropping

If the denominator is not zero and FPm is less than a chosen threshold TH_FP (TH_FP < 1) but not zero, the attack is detected as Random Packet Dropping and node m is identified as the attacker. TH_FP is chosen so that 1 - TH_FP is equal to upper bound of the dropping rate that can be tolerated.

3) Selective (Random) Packet

LFP (Local Forward Percentage) LFPs m =packets from s actually being forwarded → (2) packets from source s to be forwarded If the denominator is not zero and the statistics is zero (un-conditional dropping), the attack is unconditional Packet Dropping targeted at s. Likewise, if the LFP is less than TH_LFP (TH_LFP < 1), the attack is random Packet Dropping targeted at s. In either case, m is identified as the attacker, as shown in Fig. 3

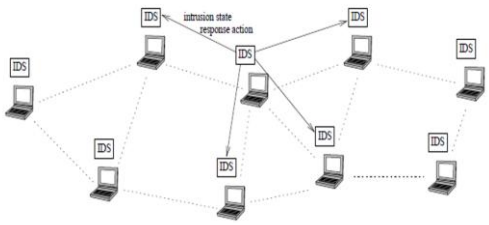


Fig. 3. Example of a selective Random Packet

4) Black hole Monitor the statistics GFP (Global Forward Percentage)

GFPm as the ratio of the total number of packets that are received by M and M should forward to the total number of packets sent by M's 1-hop neighborhood (N (M)) and are not Applications destined for another neighbor or M over a time period of L.. If all such packets are being absorbed by M for a sufficiently long period, or more precisely, if the denominator is not zero and GFP = 1, then an black hole is detected and M is identified as the attacking or misbehaving node. The detection of black hole may be infeasible if M is malicious and the attacker has total control of M so that the detection modules can be disabled.

2.2. ***Detecting attack1***

mIDS makes the following assumption to detect ATTACK1.In mobile ad-hoc networks; the transmission time is divided into contention period and transmission period. Nodes in a multi-hop wireless network use TDMA/S-TDMA to reserve a slot for transmission channel before initiating a flow. Each node gets a chance to transmit at least once during a frame time. A security mechanism can be found where a node has to digitally sign before reserving the slot. Hence the intruders cannot reserve the slot. If there is not enough bandwidth, new flows should not be admitted so that existing flows are not choked. This enables existing flows to achieve their desired Qos. After the contention period, the nodes are allowed to transmit in the same order of their reservation. An intruder may attack a node X and allow it to misbehave. Due to this misbehavior, the performance of the network decreases. Hence a node X after completion of transmitting in its slot time, have to send a special packet identifying its completion of transmission. The predecessor of node X overhears this. If the predecessor node do not hear this special packet after a duration time from X, thinks that X is misbehaving and increments the misbehaving count by one. If the misbehaving count reaches to certain threshold value, then the X is identified as a misbehaving node. The neighbors of node X are reported of this misbehaving node Alternatively let us assume that for each period T, a node X knows that p% of the available link capacity has been allocated by its neighboring nodes where p = L where L is the total link capacity. L should be less than 100% since no system can work at 100% capacity. Now for each period T, X measures the percentage of link capacity r% being used by the neighboring nodes for the admitted flows. It also measures the percentage of link capacity s% being wasted due to collisions, garbage data and flows that did not reserve bandwidth. If (r + s) >= L → (3) X assumes that, a neighbor or a group of neighbors is accessing the channel unfairly. X increases a non-negative misbehavior counter m_c each time X detects ATTACK1 and decrements it if there is no such misbehavior. If m_c reaches a threshold, X declares its neighborhood misbehaving. Sometimes a neighbor of X may not utilize the whole part of link capacity allocated to an admitted flow. This can happen if the flow does not send packets at a constant bit rate. Hence, r can be less than p. Therefore, r < p does not mean that neighbors are not getting fair share of the channel. However, r < p can also be true if a neighbor does not get fair share of the channel, as shown in Fig. 4

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

ATTACK MODEL

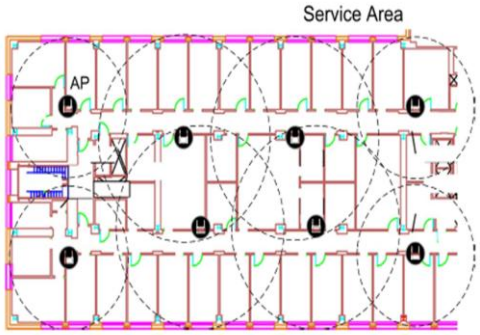


Fig. 4. Example of an Attack Model

2.3 *Detecting attack2*.

Each node measures the rate Rt [f, h] at which it processes packets, where h denotes the hop distance a node is away from the source. The destination finds the Rt [f, h=destination] and adds it to the a packet and sends it to the source through all the intermediate nodes off. Each intermediate node appends the rate to RSP and the Rt [f, h] can be digitally signed by its respective node. When RSP reaches the source node, it contains R [f, h] values of all the downstream nodes off. Now we can estimate the forwarding ratio of a node h hops away from the source by the following expression: Forwarding ratio,

F [f, h] =R [f, h + 1] / R [f, h - 1] → (4)

If Delivery ratio,

R [f, h = destination] / R [f, 0] < R thres [f] → (5)

Where R thres [f]

is the allowable minimum end-to-end delivery ratio for the flow f, the source suspects the intermediate node, h hops away from the source with the highest F [f,h], is dropping packets at an intolerable rate. The source Nodes towards the destination of a flow are called the downstream nodes. Forwarding ratio = Data received by the neighboring downstream node/Data sent from the neighboring upstream node Delivery ratio = Data received successfully/Data Sent If the misbehavior counter MBC [ATTACK2a, f, h] for each downstream node reaches a threshold, the source declares that node to be misbehaving. The packet dropping can also be detected through contact scheduling. Contact scheduling is assumed while proposing a solution for mIDS. That is a node before transmitting knows the address of all the nodes in the path to the destination. Using this path a node transmits the data. The source node encrypts the message in such a way that the decryption is possible only for the destination node and not to the intermediate nodes. The size of the onion should not be revealed to the nodes. Each time the node decrypts the message using its public key, the size of the onion is decremented. as shown in Fig. 5

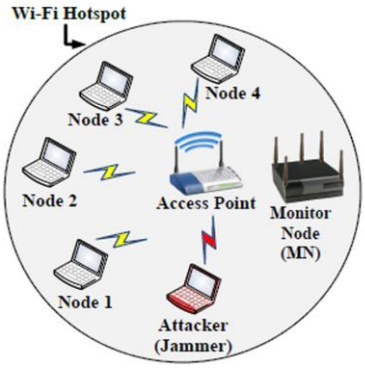
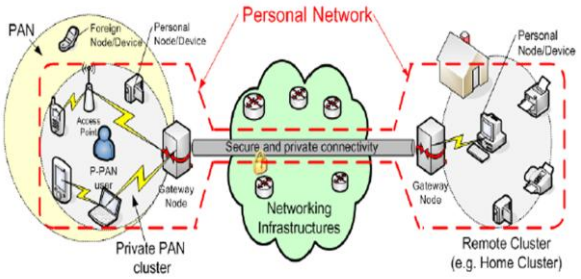


Fig. 5. Example of an Attack Model

2.4. *Monitor identification method.*

The mobile ad-hoc network is organized as a collection of such sets and each set has a monitor node. Each monitor node performs intrusion detection. There are many set-based intrusion detection schemes and set formation algorithms. Set formation using various algorithms in 18-node topology (Head Nodes are shown in Red, Gateway Nodes in Yellow and Member Nodes in Black),as shown in Fig. 6



n as
rmer
ork.

On the other hand, in the end-host reaction scheme, each node may make its own decision on how to react to a malicious node. Global reaction. The reaction scheme in falls into the global reaction category. It is based on the URSA certification framework. Once multiple nodes in a local neighborhood have reached consensus that one of their neighbors is malicious, they collectively revoke the certificate of the malicious node. Consequently, the malicious node is isolated in the network, as it cannot participate in the routing or packet forwarding operations in the future. End-host reaction.

4.1. PROPOSED MECHANISM

As explained in the address registration process is necessary to avoid the layer-two address layer resolution and to guarantee the node's IP address uniqueness. Depending on the routing approach, two different procedures can be used to perform the address registration. In the mesh-under routing approach, the nodes exchange the NS and the NA messages with the edge router. In the route-over routing approach, the process is similar to the one for mesh-under between the nodes and the 6LRs and, additionally, the 6LR uses the

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

new DAR and DAC messages to verify the address uniqueness on the edge router. Note that the current 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. We propose the use of the 8 bit length reserved fields of both cases to implement the security mechanism.

The new information to be included on this field is:
i) The transport-layer protocols which are to be accepted,
ii) The reach ability acceptance from the Internet, and
iii) The maximum Internet clients request rate shape limit.
The proposed format for the new ARO and DAR messages. New address registration option (ARO) and duplicate address request (DAR) message formats.

As shown in the table:

Filtering database fields	**ARO message fields**	**DAR message fields**
IP address(128 bits)	EUI-64	Registered address
Lifetime (16 bits)	Registration Lifetime	Registration lifetime
Accepted data from Internet layer protocol (2 bits)	Accept data from Internet	Accept data from Internet
Accepted transport layer protocol (2 bits)	Accepted transport layer protocol	Accepted transport layer protocol
Rate request limit (4 bits)	Rate request limit	Rate request limit

As shown in the table:

Field	**Length**	**Values**	**Description**
AFI	2 bits	0000	Not used
		0001-1111	Rate Limit value
		00	Not used
		01	Do Not Accept packets from the Internet
		10	Accept packets from the Internet
		11	To be defined
TP	2 bits	00	Not used
		01	UDP
		10	TCP
		11	Accept any

Field Length Values Description

Address registration option (ARO) and duplicate address request (DAR) new data fields. 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, according to the correspondence defined (Accept data from the Internet), the accepted transport layer protocol (Accepted transport layer protocol) and the Internet client rate request limit (Rate request limit)

4.2. *Filtering database fields ARO message fields DAR message fields*

IP address (128 bits)
EUI-64 Registered address Lifetime (16 bits) Registration lifetime Registration lifetime Accept data from Internet (2 bits)Accept data from Internet Accept data from Internet Accepted transport layer protocol (2 bits) as shown in Fig 8.

Client IP address (128 bits)	**Lifetime (16 bits)**	**IP destination address (128 bits)**	**Rate request (4 bits)**	**Rate request Limit (4 bits)**

Fig. 8. Example of fixed length values

Accepted transport layer protocol Accepted transport layer protocol Rate request limit (4 bits) Rate request limit Rate request limit **Filtering** database fields correspondence. The Internet client address table is used for ensuring that no Internet client generates address must remains in the blacklist (Lifetime), IP address of the destination node (IP destination address), and the number of times that this address was added to the blacklist (Counter). The Lifetime value must be increased if the same client IP address repeats several times for the same or for different destination address. So, the blacklist table entries should not be removed after the lifetime goes to zero. As shown in the Fig.9.

Client IP address (128 bits)	**Lifetime (16 bits)**	**IP destination address (128 bits)**	**Counter**

Fig.9. An Example of Filtering fields

4.3. *Filtering Packets Received from the Internet*

When the edge router receives a packet from the Internet destined to an address of the smart object network, it must first verify if the destined address exists, if the destination node accepts the transport layer protocol of the packet and if the packet IP source address is not present in the Internet client blacklist table with lifetime value greater than zero. Internet client´s address and Internet client blacklist tables are updated for each packet received from the Internet.

A. 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 and packets being

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

discarded. 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.

B. 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. Even after the packet is sent out by *A*, *B* may not be able to decode it correctly, due to the interference introduced by *X*. Such a scenario is an unsuccessful delivery. The PDR may be measured at the receiver *B* by calculating the ratio of the number of packets that pass 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.

5. CONCLUSION

DoS and DDoS can be done locally and remotely, and it is one of the most common types of security attacks, because it requires only regular and inexpensive resources, and does not require high technical knowledge. The frequency and sophistication of DoS and DDoS are rapidly increasing based on several techniques including direct attacks, remote controlled attacks, reflective attacks, worms, and viruses. The proposed security mechanism prevents smart object networks from remotely initiated DoS (and DDoS) network and transport layer attacks. The mechanism filterers unwanted traffic originated on the Internet and destined to the smart object network nodes and it is based on the address registration process protocol mechanism, the traffic is forwarded from the Internet to the smart object networks only if it is in accordance with the following rules:

• Nodes should previously inform the edge router about the accepted traffic rate limit; in fact, in most sensor cases, measurements data is generated at a slow acquisition rate (for example, air temperature monitoring), which puts a limit on acceptable request rates preventing, in this way, flooding attacks. To implement the proposed mechanism, it is only necessary to define three fields in ARO and DAR messages. The proposed mechanism uses stateless traffic processing, so it can run simultaneously in different edge routers, providing more robustness to the network. In the original ARO and DAR messages, the zeros are used to fill the reserved data fields. As a consequence, the compression rates are not compromised Authentication and client puzzles based mechanisms can be used in the edge router to provide a more coarse traffic admission control. Adding authentication, client puzzle mechanisms to the current solution, providing more application- based control and conducting a performance evaluation in real scenarios will be addressed as future work.

REFERENCES

[1] F. Anjum, D. Subhadrabandhu and S. Sarkar. Signaturebased intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

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

[3] Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

[4] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008)

[5] Giriraj Chauhan,Sukumar Nandi: QoS Aware Stable path Routing (QASR) Protocol for MANETs, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[6] Xiapu Luo, Edmond W.W.Chan, Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)

[7] Ponomarchuk, Yulia and Seo, Dae-Wha, "Intrusion Detection Based On Traffic Analysis in Wireless Sensor Networks" IEEE 2010. [8] S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

BIOGRAPHY

Chilakalapudi Meher Babu is pursuing is M.Tech in Nimra Institute of Science And Technology affiliated to Jawaharlal Nehru Technological University, Kakinada, and A.P. INDIA. His research areas comprise CISCO Packet Tracer and Computer Networks.

Dr. Ujwal A. Lanjewar, Ph.D., MCA, M.Sc. (Stats), MBA, Diploma in Industrial Engineering, Diploma in Export Management, is a Professor and Research Supervisor in the Faculty of Computer Science of R.T.M. Nagpur University, Nagpur. He was awarded as **"Professor Raghvendra Rao Best Application Paper Award"** in International Conference, 37th Annual Convention of ORSI held at IIM, Ahmadabad during Jan 8-11, 2005.

Chinta Naga Manisha did her M.Tech in Computer Science and Technology in 2009 from GITAM University, Visakhapatnam. A.P. INDIA. Her area of expertise includes Computer Networks, Information Security and Cloud computing. She is working as Assistant Professor in department of Computer Science and Engineering Technology at Nimra Institute of Science And Technology, Vijayawada, Andhra Pradesh, India.