ISSN 2277-3061

Performance Analysis of Malicious nodes on Multi hop Cellular Networks

G. Vidhisha Yadav*
M Tech (CSE)
N. Ramanjaneya Reddy
Asst Prof in CSE
U.Sesadri
HOD of CSE
vidhisha.biotech@gmail.com

Abstract

The existence of malicious nodes in multi hop cellular networks, which operate without a central administration infrastructure, can result in performance degradation or even disruption of the network operation. In this paper we proposed some approaches to analysis the consequences caused by malicious nodes in networks. We analyzed and reported the simulation result, that the effect on performance of network when malicious node present in it. Based on our past report on the behavior of all nodes we will achieve higher levels of security and reliability by utilizing them. To reduce the public key cryptography operations we will use light weight hashing operations along with the routes between source and destination.The proposed model improves all the drawbacks of multi hop cellular networks, which excludes and if not possible, minimizes the number of malicious node in the routes.

Key words: Network-level security and protection, payment schemes, Ad-hoc networks, malicious attacks.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol. 11, No. 7
editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. INTRODUCTION

In wireless Ad-hoc networks there is no central management infrastructure but they will communicate through a group of wireless devices. There are many advantages with this a capability, along with the mobile nature of these networks. However, these same characteristics are the root of several nontrivial challenges in securing such networks. The nodes will move freely and organize themselves in a capricious fashion in these networks. Multi hop routing capability is required to communicate nodes but not in radio range. That is, each node may need to act as a router, forwarding packets to other nodes. Whenever infrastructure is not available then this type of networks will be used in wide range of applications. Based on the deployment feature it will be used mainly in military fields, disaster and rescue operations, conferences, as well as home and mesh networking.

In networks the major challenge is lack of security. For trust worthy this type of networks have only few trusted and limited users by changing the topology to open the architecture of network constantly since the ability is that both guanine and malicious attackers can access this wireless channel. Also, the lack of any centralized architecture or authority, can limit the use of many conventional security solutions, such as those based on traditional public key infrastructure, which are designed around a centralized mechanism. Whenever the node is refused to forward data packets then it will be treated as misbehavior in networks. In some circumstances, the node can be overloaded, which affects the CPU cycles, buffer space, and available bandwidth to forward packets. Nodes have also been known to save available resources by not forwarding packets unless they are of direct interest to the node itself. Conversely, these nodes may still be expecting others to forward packets on their behalf [4].

To manage and store node accounts AC central bank is used to eliminate the need for TPDs.For each transmitted packet the source node appends the payment node and intermediate node checks whether the token belongs to a winning ticket or not by using its secret key. To get the reward winning tickets are sent to AC. The immediate nodes are rewarded per winning tickets while the source and destination packets are charged per packet. In a security flaw, the colluding nodes can exchange tokens to be checked in eachnode to steal credits. In our earlier work, instead of submitting payment checks to the AC, each node submits an activity report containing its alleged charges and rewards of different sessions. The AC uses a reputation system to identify the cheating nodes that report false charges and/or rewards to steal credits. However, due to the nature of the reputation systems, some honest nodesmay be falsely identified as cheaters and the colluding nodes may manage to steal credits.

In each node in a route buys packets from the previous node and sells them to the next node. Linu Ann Joy at el, the packets buyers contact the AC to get deposited coins and the packets' sellers submit the coins to the AC to claim their payment. However, the interactive involvement of the AC in each communication session is not efficient and creates a bottleneck at the AC. In [4], an incentive mechanism has been proposed for MCN. Unlike the original MCN architecture proposed in [5], the base stations are involved in every communication session, which may lead to suboptimal routes when the source and destination nodes reside in the same cell. In addition, the corrupted messages are relayed to the base station before they are dropped because the intermediate nodes cannot verify the authenticity and the integrity of the messages.

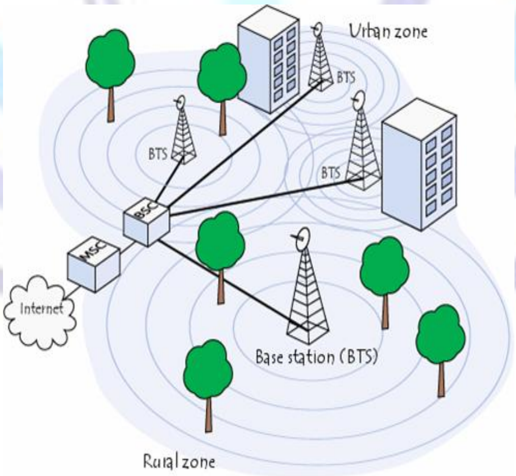


Figure 1 Multihop Cellular Networks Architecture

In Sprite [6], the source node appends its signature to each transmitted message the signs is done on the identities of the nodes in the route. The intermediate and the destination nodes compose checks and submit them to the AC to claim the payment. In Express [7], the source node generates a hash chain for each intermediate node IDK and commits to the hash chain by digitally signing the root of the hash chain and sending the signature to IDK. Each time the node IDK relays a message, the source node releases the pre image of the last sent hash value. The checks are composed and submitted to AC by source, intermediate, and destination nodes.

Due to node mobility any node may interact as intermediate node in networks so it must generate and store high number of hash chains. The source node has to attach one hash value for every intermediate node, so it suffers from packet overhead. In Sprite and Express, only the source node pays no matter how the destination node benefits from the communication. In Mohammed et al., Moreover, since the intermediate nodes are rewarded for the relayed messages that do not reach the destination, allthe nodes in a route submit the checks because packet relay is considered successful by a node if a next node in the route submits a valid check. We call this check submission scheme All Submitters because all the intermediate nodes submit all the checks. In Sprite and Express, significant communication and computation overhead is implied due to generating and submitting a large number of checks because a check is generated per message and all the nodesin a route submit all the checks.

In adhoc networks to connect nodes in internet, an incentive mechanism has been proposed. In Mohammed E et al., The source node signs the identities of the nodes in the route and appends this signature to the message, and the destination node signs a check and sends it to the last intermediate node to submit to the AC. Since only the last intermediate node submits the check, we call this check submission scheme Fixed-Submitter. In Mohammed MEA et al., However, the source and destination nodes can communicate freely and the intermediate nodes are not rewarded if the last intermediate node colludes with the source and destination nodes to not submit the checks. Moreover, generating two signatures per message is too costly for mobile nodes. A hash chain is used to efficiently authenticate digital streams but FESCIM uses a hash chain to achieve payment non repudiation to secure the payment.

2. SECURITY DEFICIENCIES IN CELLULAR NETWORKS

Strictly speaking, although the term is usually used to refer to a node that attempts to disrupt, destroy or destabilize a network, a malicious node is any node that weakens or reduces a network’s capability to perform its expected function [6].

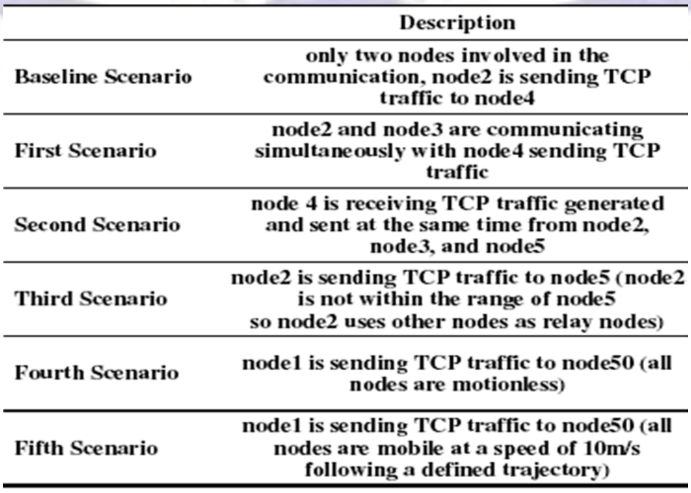
Identifying the most popular malicious attacks in Ad-hoc networks is the first step towards the development of any trust evaluation system. One simple form of malicious node is one that drops packets. This node can still participate in lower-level protocols, but it drops packets on a random basis. This causes the quality of the connections to become aggravated and can further have a negative effect on the performance if TCP is the transport layer protocol used [7]. Forwarding messages alongwrong paths is another form of malicious nodes. These nodes tend to divert packets away from their intended destination, which may lead to a DoS attack. Malicious nodes can also fabricate and transmit falsified routing messages to mislead other routes and to create invalid paths in their routing tables.

These types of nodes advertise false routing messages to every other node, forming a black-hole and a wormhole within the network [8]. As their advertisement propagates, the network routes more traffic in their direction. The effects could lead to route failures and thus affect the overall performance of theAd-hoc network. A malicious node can launch a replay attack by sending stale updates to some node, in an attempt to get that node to update its routing table using out of date routes. This can also lead to degradation in the performance of the Ad-hoc network.

3. BEHAVIOR OF THE NETWORK NODES

In the proposed scheme, the source node tends to find a route to the destination that enclose less number of malicious nodes as opposed to the traditional protocols that aim to choose the shortest route. To achieve this, a new parameter is added to the routing protocol to record the behavior of a node. This parameter is a function of the packets relayed by this node. These include control packets as well as data packets. In the first phage, this parameter is same for all nodes. Every time a node forwards either data or control packet, the parameter is incremented. Conversely, whenever a node fails to relay a packet, the parameter is decremented. Therefore, the more packets forwarded by a node the more reliable this node will be. This level of reliability allows this node to be chosen by other nodes.

On the other hand, the fewer packets a node forwards, the less trusted this node will be and thus will not be used to forward packets to other nodes. When a node wants to communicate with another node, it finds a set of routes to the destination using one of the on-demand routing protocols. The source node then forwards the packet to the neighbor node with the highest value of the behavior parameter. In the case where two neighbor nodes have the same behavior value, the source will choose the node corresponding to the route with the less number of hops.



	Description
Baseline Scenario	only two nodes involved in the communication, node2 is sending TCP traffic to node4
First Scenario	node2 and node3 are communicating simultaneously with node4 sending TCP traffic
Second Scenario	node 4 is receiving TCP traffic generated and sent at the same time from node2, node3, and node5
Third Scenario	node2 is sending TCP traffic to node5 (node2 is not within the range of node5 so node2 uses other nodes as relay nodes)
Fourth Scenario	node1 is sending TCP traffic to node50 (all nodes are motionless)
Fifth Scenario	node1 is sending TCP traffic to node50 (all nodes are mobile at a speed of 10m/s following a defined trajectory)

Table 1: Description of Scenarios used

The source node then checks if the corresponding node forwards the packet or drops it using the promiscuous capability of the wireless cards. In the first case the behavior parameter of this node will be incremented otherwise it ends up being decremented. The different aspect of this scheme when comparing it to the scheme in the node does not wait to receive an acknowledgment sent by the destination in order to update the behavior parameter. Instead the update is done after the node forwards the packet. This specific technique solves the problem of not receiving the acknowledgment which may occur due to varying reasons. In this case the whole route will get a negative behavior for a reason which is not caused by a malicious attack. Further if an intermediate node drops the packet, it will not affect all the nodes in the corresponding route. This process is repeated until the packet reaches the destination node. It should be noted here that the possibility of an intermediate node forwarding the packet to a third node that is not a part of the route to deceive the originator node is not considered.

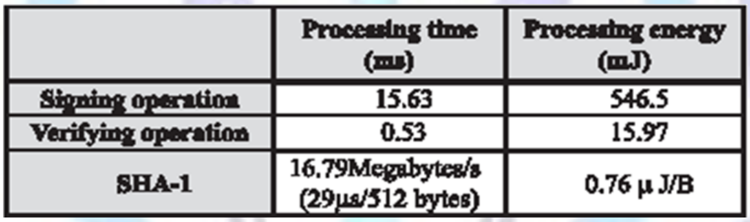
4. PERFORMANCE EVALUATION

In this phage we will evaluate the checks' overhead in terms of the check size and the number of generated checks. We alsoevaluate the overhead of the signed and hash-chain-based ACKs in terms of energy consumption and end-to-endpacket delay.

4.1 Simulation Setup

In our simulation, we consider the RSA signature scheme and SHA-1 hash function with digest length of 20 bytes. Although the signature tags of the DSA and ECDSAsignature schemes are shorter than that of the RSA, theseschemes increase the end-to-end delay significantly becausethe verifying operations performed by the intermediate anddestination nodes are computationally more demandingthan the signing operations performed by the source node. It is shown that the verification time of the 1,024-bitRSA is more than 31 and 45 times faster than those of the168-bit ECDSA and 1,024-bit DSA, respectively, and thesignature generation is measured to be around 8 and 6 timesslower. According to NIST guidelines, the secureprivate keys should have at least 1,024 bits.

In order to estimate the computational processing timesfor the signing, verifying, and hashing operations, we haveimplemented 1,024-bit RSA and SHA-1 using the Crypto++ library. The mobile node is a laptop with an Intelprocessor at 1.6 GHZ and 1 GB Ram, and the operatingsystem of the mobile node is Windows XP. The resultsgiven in Table 3 indicate that the RSA signature generationis computationally intensive but the signature verificationis much faster. The energy consumption of the RSASHA-1 operations is measured the results. The resources of a real mobile node maybe less than a laptop, so the results given in Table 3scaled by the factor of 5 in our simulations to estimatelimited-resource node.



	Processing time (ms)	Processing energy (mJ)
Signing operation	15.63	546.5
Verifying operation	0.53	15.97
SHA-1	16.79Megabytes/s (29µs/512 bytes)	0.76 µ J/B

Table 2: Processing times and Energy for RSA and SHA-1

We did the simulation on the 1000m to 1000m square cell of an MCN. Thirty five mobile nodes are deployed randomly and a base station fixed at centre of the radio transmission range of the mobile nodes andbase station is 125 m. to evaluate nodes mobility we used the modified random waypoint model. Specifically, a node travels toward a random destinationuniformly selected within the network field, upon reachingthe destination, it pauses for some time; and the processrepeats itself afterward. The node speed is uniformlydistributed in the range ½0; Smax m/s and the pause timeis 20 s. The constant-bit-rate traffic source is implementedeach node as an application layer.

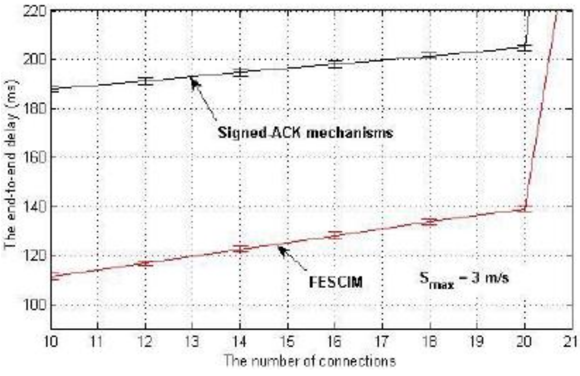


Figure 2end-to-end delays for the signed ACK mechanisms and FESCIM.

The source and destination pairs are selected randomly. All data packetshave 512 bytes and are sent at the rate of 0.5 packets/s.simulate the dynamic source routing (DSR) protocolover distributed coordination function of the IEEE 802.11medium access control protocol. The time stamp, node'sidentity, and the number of messages are 5, 4, and 2 bytes,respectively. Network simulator NS2 (version 2.27)used to evaluate the end-to-end delay and the networkthroughput using signed and hash-chain-based ACKs,MATLAB is used to evaluate the check overhead.Simulation is executed for 15 simulated min and each datapoint represents the average of 50 runs.

5. RESULTS AND ANALYSIS

All simulations run for five minutes. TABLE II shows the throughput variation values collected at node2 and when 40% of the nodes are acting maliciously. This table shows bothsituations where the malicious nodes are sending UDP and TCP traffic. It is clear from these values that the impact on the throughput is less when the malicious nodes are using UDPtraffic rather than TCP traffic. This is attributed to the nature of TCP, which ensures that the data is delivered error free and in order. As the receiving node does not distinguish between malicious and data traffic, delays at node2 can be expected. This is in line with previously published results [4].

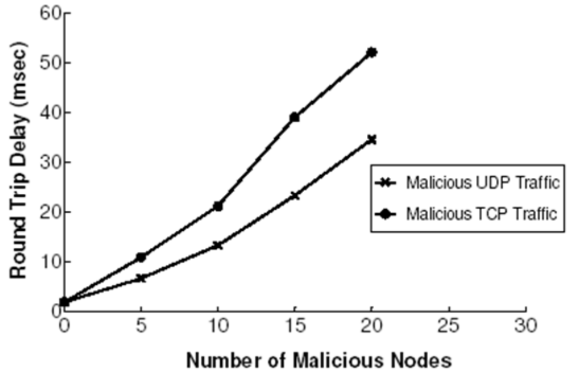


Figure 3 round trip delay variation for base line scenario measured at node2 for TCP and UDP malicious traffic

The graphs in Figure 2 show the round-trip delay variation for the baseline scenario. Again, the measurement is made at the sending node and the graphs show both situations where the malicious nodes are sending UDP and TCP traffic. It is noticeable from these graphs that the malicious nodes have affected the round-trip delay between the communicating nodes for this scenario. These graphs also indicate that the impact on the round-trip delay is less when the malicious nodes are using UDP traffic.

This can be attributed to the use of the window mechanism to control the flow of data in TCP. When the establishment of TCP connection is fired, each end of the connection has buffer to hold incoming data. The receiver wilI send a ACK with positive window advertisement if it can read data as quickly as it arrives. Kurose and Ross at el.However, as expected if the sender is faster than the receiver, incoming data will eventually fill the receiver's buffer. Thus, asdata and malicious traffic arrive at node2, node2 sends acknowledgements to each node causing delay and full buffer at node2. In this situation node2 advertises a zero window. Until receiving a positive window, the sender receives a zero window advertisement.

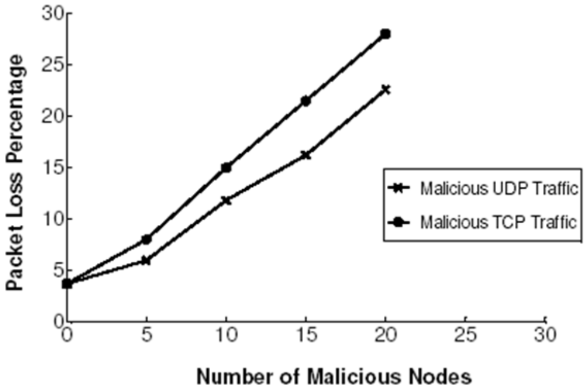


Figure 4 packet loss percentage for the 1^{st} scenario measured at node 2 for TCP and UDP malicious traffic

The graphs in Figure 3 show the packet loss percentage variation for the first scenario. Also the graphs show the situations of both UDP and TCP traffic sent by the malicious nodes.Based on these graphs we can say that the presence of malicious nodes causes the packet loss rate in the network. Additionally, this is in line with previously published results. These graphs also show that this performance metric is also plagued by the transport protocol that the malicious nodes are using. The malicious nodes are when using TCP, they will try to re transmit their traffic this is an attributed fact. This process at nodes2 cannot distinguish between normal and malicious traffic. So this can cause higher packet loss rate compared to when malicious nodes are using UDP. The performance of the baseline, second and third scenarios also shows similar behavior to the first scenario. For example, the packet loss rate has risen from 0 toaround 10% when twenty malicious nodes using UDP protocol are present in the network, compared to 15% when using TCP for the baseline scenario.

OPNET Modeler provides several statistics during simulation execution to analyze the performance of the routing protocol used. The available AODV performance statistics Total Route Request Sent, Total Route Replies Sent, Total Route Errors Sent, Total Replies Sent from Destination, Total Packets Dropped, Total Cached Replies Sent, Routing Traffic Sent (Packet/Second), Routing Traffic Received (Packet/Second), Number of Hops Per Route, and Packet Queue Size.

Routing Traffic sent defines the total number routing traffic sent in packets in the entire network. This statistic was collected to check the amount of routing trafficgenerated by the network when using the proposed BAODV protocol as the routing protocol. It is noticeable these graphs that the amount of routing traffic sent in the entire network is higher when using the BAODV protocol. This due to the fact that when a malicious node between a source and a destination node is detected, the routing path between these two nodes will change causing an increase in the routing traffic.

6. CONCLUSIONS

The route is established through exclusion of the nodes that may be considered to be malicious,based on their behavior. The results of throughput, round-trip delay, and packet loss rate, with some nodes acting maliciously have been studied. Data collections for different situations, where malicious nodes are sending TCP and/or UDP traffic are also carried out. Simulation studies, using OPNET, demonstrate that the malicious nodes sending UDP traffic have less negative impact on the overall performance of the network compared to when they send TCP traffic. The reported results clearly show that the overall performance of the networks, even in the presence of malicious nodes, can be significantly improved by incorporating the behavior of the nodes. For instance, with 40% of the nodes of the network acting maliciously, and nodes being eitherstationary or mobile, increases of 11% and 13% respectively in throughput values can be achieved.

REFERENCES

[1] S. Dhar, "MANET: Applications, Issues, and Challenges for theFuture," International Journal of Business Data Communicationsand Networking, 2005, vol. 1, pp. 66-92.

[2] K. S. Ng and W. K. G. Seah, "Routing security and dataconfidentiality for mobile Ad-hoc networks," In Proc. of the 57thIEEE Semiannual Vehicular Technology Conf. (VTC 2003-Spring),2003, pp. 1821-1825 vol.3.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobileAd-hoc networks: challenges and solutions," WirelessCommunications, IEEE, 2004, vol. 11, pp. 38-47.

[4] A. S. Marti, A. T. J. Giuli, A. K. Lai, and A. M. Baker, "Mitigatingrouting misbehavior in mobile Ad-hoc networks," In Proc. of the6th Int. Conf. on Mobile computing and networking, Boston,Massachusetts, United States, 2000, pp. 255-265.

[5] H. Hallani and S. A. Shahrestani, "Performance Evaluation andSimulation Verification for Wireless Ad-hoc Networks," WSEASTransactions on Communications, 2005, vol. 4, pp. 355-362.

[6] A. D. Wood and J. A. Stankovic, "Denial of service in sensornetworks," Computer, 2002, vol. 35 No.10, pp. 54-62.

[7] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of ServiceAttacks at the MAC Layer in Wireless Ad Hoc Networks,"MILCOM, 2002, pp. 1118-1123.

[8] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficientdistance vector routing for mobile wireless ad hoc networks," InProc. of the Fourth IEEE Workshop on Mobile Computing Systemsand Applications (WMCSA'02), 2002, pp. 3-13.

[9] Y. Hu, A. Perrig, and D. Johnson., "Ariadne: A secure on-demandrouting protocol for Ad-hoc networks," Wireless Networks, 2005,vol. 11, pp. 21-38.

[10] A. I. Aad, A. J.-P. Hubaux, and A. E. W. Knightly, " Denial ofservice resilience in ad hoc networks," In Proc. of the Proceedingsof the 10th annual international conference on Mobile computingand networking, Philadelphia, PA, USA, 2004, pp. 202-215. Report TR-050111, Computer Science Dept., Florida State Univ., Jan. 2005.

[11] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, “Cooperation Enforcement Schemes for MANETs: A Survey,” J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332, 2006.

[12] C. Song and Q. Zhang, “OMH-Suppressing Selfish Behavior in Ad Hoc Networks with One More Hop,” Mobile Networks and Applications, vol. 14, no. 2, pp. 178-187, Feb. 2009.

[13] D. Djenouri and N. Badache, “On Eliminating Packet Droppers in MANET: A Modular Solution,” Ad Hoc Networks, vol. 7, no. 6, pp. 1243-1258, Aug. 2009.

[14] G. Bella, G. Costantino, and S. Riccobene, “Evaluating the Device Reputation Through Full Observation in MANETs,” J. Information Assurance and Security, vol. 4, no. 5, pp. 458-465, Mar. 2009.

[15] L. Feeney, “An Energy-Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks,” Mobile Networks and Applications, vol. 3, no. 6, pp. 239-249, 2001.

[16] M. Peirce and D. O’Mahony, “Micropayments for Mobile Networks,” technical report, Dept. of Computer Science, Trinity College, 1999.

[17] L. Buttyan and J. Hubaux, “Enforcing Service Availability in Mobile Ad-Hoc WANs,” Proc. ACM MobiHoc, pp. 87-96, Aug. 2000.

[18] L. Buttyan and J. Hubaux, “Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks,” Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct. 2004.

Author Profiles:

Mrs G Vidhisha Yadav received her B.Tech in Bioinformatics from MITS-Madanapalliand now pursuing M.Tech (CSE) Vaagdevi Institute of Technology and Sciences,JNTU-Anantapur.

Mr N Ramanjaneya Reddy received his M Tech in CSE and working as a Asst Prof in CSE in Vaagdevi Institute of Technology and Sciences, under JNTU-Anantapur.

Mr.U.Seshadri received his M.Sc (CS) from SriVenkateswara University-Tirupati, M.Tech (CSE) from Satyabhama University. Working as HOD in CSE in Vaagdevi Institute of Technology and Sciences, under JNTU-Anantapu.