Secure routing in Mobile Ad hoc Networks: Laurel verification based Node Selection Strategy

K Sreenivasulu[1] , Dr E V Prasad [2] and Dr A subramanyam[3]
[1] Department of Computer Science and engineering
Madina Engineering College KADAPA, A.P. INDIA

[2] DIRECTOR & Professor in Computer Science and Engineering
Lakireddy Balireddy College of Engineering MYLAVARAM. VIJAYAWADA A.P INDIA

[3] Professor & HOD of Computer Science and Engineering
AITS, Rajampet KADAPA. A.P INDIA

Abstract

As the nodes are self resourced in ad hoc networks, the denial of service as relay hop by any node is frequent. This is due to resource levels of that node are lower than the threshold, in another act the node may be irrational and selfish. In such cases the irrational or selfish nodes leads to attacks such as black-hole and grey-hole and also causes the poor routing performance under metrics such as throughput, Packet Delivery Ratio and Packet Delivery Fraction. In this paper, deviced a node laurel verification and update strategy to avoid irrational and selfish nodes from network activities. The laurel verification is done in between periodic intervals and laurel update incorporates at routing completion state. We conducted experiments using simulations build by NS-2, which are promising and optimistic over models stated in recent literature.

Keywords: MANET, AODV, laurel, trust, routing

1. INTRODUCTION

Due to the extremely high mobility of the nodes in an ad-hoc network environment, a centralized authority based security make normal security options structural. Most of the existing dispersed laurel based security protocols for ad-hoc networks examined in networks with potentially low or no mobility and dependents of scenarios such as extending node halt time and decelerating node mobility [1][4][5][18]. The approach of selfish node detection by a watch dog approach is devised in [7]. Monitoring neighbor nodes and identifying their malicious behavior by adaptive Bayesian laurel can be found in [8]. Detecting nodes with malevolent behavior by the process of mutual Localized voting s devised in [5], which is a network layer security protocol. Eigen Trust protocol is another model devised in [9] that gives each node a distinctive trust rating, based on the node's earlier track of transactions. Eigen Trust (1 or -1) is allotted by the relay hop nodes, which is based on the responsiveness of the targeted node. Other experiments attempted to provide routing level methods to black-hole attacks, with techniques to identify and separate these nodes as in [10][11]. [10] Recommended that a node communicates with one additional node while [11] considered static sensor networks which are not much like MANET problems. The model devised in [12] explored a solution against collaborative black hole attack. This model is using next hop information agreement but showed no effects or detailed analysis.

Here in this paper we projected a laurel based self ordered process that's specifically targeted for ad hoc networks with sparse nodes with extremely high mobility. The proposed model is centric of disseminated laurel tips, which can be found in [2] and aims to achieve optimal speed in seclusion of nodes with malevolent behavior.

The rest of the paper is organized as follows. Section 2 describes our proposed protocol, section 3 is exploring the experimental results and Section 4 concludes and determines future work.

2. NODE LAUREL VERIFICATION AND UPDATE

In proposed model, each node should equip with Laurel State Update (LSU) Functionality. The LSU capable to update the laurel thresholds defined for any node of the network. Each node exposes three laurel thresholds labeled as Laurel as Source (LS), Laurel as Destination (LD), Laurel as Relay (LR). The laurel of the node as source represented by LS, as destination represented by LD and as relay node represented by LR. The default initial values of these thresholds of each node are 0 (zero). The thresholds labeled as NDST, NDDT and NDRT represents Network level denial as Source Threshold, Network level denial as Destination Threshold and Network level denial as Relay Threshold respectively. The briefing of proposed approach is following

The following sections elaborates the approach of the proposal

2.1 Laurel Verification:

In a given time intervals,

- Set of nodes that selected as controllers estimates NDST, NDDT and NDRT.
- Verifies sensitivity of LS, LD and LR of each node in the context of NDST, NDDT and NDRT respectively.
- Nodes that are identified as irrational and selfish will be avoided from network activities

2.1.1 Selecting Controllers

Initially the geographical area spanned by nodes in target network will be partitioned into zones. A mobile agent will be used that traverse all nodes in a region to find out the state of the parameters such as available energy, permanence, and mobility. Further one of the nodes from that region, which found to be with high energy, permanence and low mobility, will be selected as controller. The approach of measuring the proportionate state of the energy, permanence and mobility is as following:

For each node n_i , where i=1...n

The energy threshold et_i is $1-\frac{1}{ne_i}$ (1)

Here in Eq.(1) ne_i energy in joules available at node n_i

The permanence threshold pt_i is $1-\frac{1}{(ne_i/ec_i)}$ (2)

Here in Eq.(2) ne_i is energy available at node n_i and ec_i is energy consumption rate per unit of time at node n_i

The mobility Threshold mt_i is $1-\frac{1}{(nm_i/ad_i)}$ (3)

Here in Eq.(3), nm_i is node mobility speed and ad_i is average distance between node current position and zone boarders.

Then controller state threshold of node n_i is found as follows

$$cst(n_i) = abs(et_i + pt_i - mt_i) \quad (4)$$

Here in Eq.(4) ' $cst(n_i)$ ' represents controller state threshold of the node n_i

Finally the node with highest control state threshold will be selected as controller of that zone. Further the selected controller of the each zone acknowledges its state to all other nodes of the same zone.

2.1.2 Measuring NDST

In periodical intervals the nodes exists in a zone informs their LS value to the controller. The controller authenticates the received LS of each node n_i by verifying the LSU stamp such that the stamp is not made by LSU of the node n_i . Then it considers the average of the LS values received from those zone level nodes as zone level LS $ZDST_i$. Then this $ZDST_i$ and $ZDST$ received from other possible controllers will be shared with it neighbor controllers. Hence every controller will have the ' $ZDST$ ' of all other controllers. Then each controller measures the average of $ZDST$ values received and considers it as $NDST$

$$ZDST_j = \frac{\sum_{i=1}^{n} LS_i}{n} \quad (5)$$

$$NDST = \frac{\sum_{j=1}^{m} ZDST_j}{m} \quad (6)$$

Here in Eq.(5) n indicates the number of nodes in zone j.

Here in Eq.(6) m indicates the number of zones in network

2.1.3 Measuring NDDT

In periodical intervals the nodes exists in a zone informs their LD value to the controller. The controller authenticates the received LD of each node n_i by verifying the LSU stamp such that the stamp is not made by LSU of that node n_i . Then it considers the average of the LD values received from those zone level nodes as zone level LD $ZDDT_i$. Then this $ZDDT_i$ and $ZDDT$ received from other possible controllers will be shared with it neighbor controllers. Hence every controller will

have the ' $ZDDT$ ' of all other controllers. Then each controller measures the average of $ZDDT$ values received and considers it as $NDDT$

$$ZDDT_j = \frac{\sum_{i=1}^{n} LD_i}{n} \quad (7)$$

$$NDDT = \frac{\sum_{j=1}^{m} ZDDT_j}{m} \quad (8)$$

Here in Eq.(7) n indicates the number of nodes in zone j.

Here in Eq.(8) m indicates the number of zones in network

2.1.4 Measuring NDRT

In periodical intervals the nodes exists in a zone informs their LR value to the controller. The controller authenticates the received LR of each node n_i by verifying the LSU stamp such that the stamp is not made by LSU of that node n_i. Then it considers the average of the LR values received from those zone level nodes as zone level LR $ZDRT_i$. Then this $ZDRT_i$ and $ZDRT$ received from other possible controllers will be shared with it neighbor controllers. Hence every controller will have the ' $ZDRT$ ' of all other controllers. Then each controller measures the average of $ZDRT$ values received and considers it as $NDRT$

$$ZDRT_j = \frac{\sum_{i=1}^{n} LR_i}{n} \quad (9)$$

$$NDRT = \frac{\sum_{j=1}^{m} ZDRT_j}{m} \quad (10)$$

Here in Eq.(9) n indicates the number of nodes in zone j.

Here in Eq.(10) m indicates the number of zones in network

2.1.5 Verifying Node State

Every controller estimates the status of the nodes in its region by their LS, LD AND LR value. If found to be irrational then it publicize that all other nodes through their respective controllers, so that the irrational nodes can be avoided from the network transactions. The irrational nodes will be found as follows

Controller initially finds the zone level irrational threshold as follows:

$$zit_j(LS) = \frac{\sum_{i=1}^{n} \{LS_i \mid LS_i < NDST\}}{\{\mid n' \mid \forall n' > 0\}} \quad (11)$$

Here in Eq.(11), $zit_j(LS)$ is the zone level irrational threshold of LS.

The numerator of the division operation is the summing of LS of nodes those less than NDST and denominator is total number of nodes with LS less than NDST

Then each controller shares their ' $zit_j(LS)$ ' with all other controllers, and upon receiving the $zit(LS)$ all other zones, each controller measures network level irrational threshold of LS as follows:

$$nit_{LS} = \frac{\sum_{j=1}^{Z} zit_j(LS)}{Z} \quad (12)$$

Here in Eq.(12), nit_{LS} is the network level irrational threshold of LS. In division operation the numerator is summing the all zone level irrational thresholds of LS and denominator Z is total number of zones.

In this similar passion zone level irrational thresholds $zit(LD)$ and $zit(LR)$ of LD and LR also measured and further network level irrational thresholds nit_{LD} and nit_{LR} of LD and LR will be measured as like as nit_{LS}. The formulation is similar to Eq.(11)and Eq.(12)

Zone level irrational threshold of LD can be measured as follows:

$$zit_j(LD) = \frac{\sum_{i=1}^{n} \{LD_i \mid LD_i < NDDT\}}{\{\mid n' \mid \forall n' > 0\}} \quad (13)$$

Here in Eq.(13), $zit_j(LD)$ is the zone level irrational threshold of LD. The numerator of the division operation is the summing of LD of nodes those less than NDDT and

denominator is total number of nodes with LD less than NDDT

Then each controller shares their ' $zit_j(LD)$ ' with all other controllers, and upon receiving the $zit(LD)$ all other zones, each controller measures network level irrational threshold of LD as follows:

$$nit_{LD} = \frac{\sum_{j=1}^{Z} zit_j(LD)}{Z} \quad (14)$$

Here in Eq.(14), nit_{LD} is the network level irrational threshold of LD. In division operation the numerator is summing the all zone level irrational thresholds of LD and denominator Z is total number of zones.

Zone level irrational threshold of LR can be measured as follows:

$$zit_j(LR) = \frac{\sum_{i=1}^{n} \{LR_i \mid LR_i < NDRT\}}{\{|n'| \forall n' > 0\}} \quad (15)$$

Here in Eq.(15), $zit_j(LR)$ is the zone level irrational threshold of LR. The numerator of the division operation is the summing of LR of nodes those less than NDRT and denominator is total number of nodes with LR less than NDRT

Then each controller shares their ' $zit_j(LR)$ ' with all other controllers, and upon receiving the $zit(LR)$ all other zones, each controller measures network level irrational threshold of LR as follows:

$$nit_{LR} = \frac{\sum_{j=1}^{Z} zit_j(LR)}{Z} \quad (16)$$

Here in Eq.(16), nit_{LR} is the network level irrational threshold of LR. In division operation the numerator is summing the all zone level irrational thresholds of LR and denominator Z is total number of zones.

And finally network level irrational threshold will be measured by each controller as follows:

$$nit = (nit_{LS} - nit_{LR}) + (nit_{LD} - nit_{LR})$$

Then controller identifies each node n_i as irrational if

$$((LS(n_i) - LR(n_i)) + (LD(n_i) - LR(n_i))) \geq nit \quad (17)$$

Finally each controller publicizes about these irrational nodes to all fair nodes of that zone and also exchange with neighbor controllers

2.2 Laurel Update

On activity of a node n_s as source, the destination node n_d updates LS of the n_s according to, how node n_d finds the node n_s as source, and node n_s updates the LD of n_d according to, how node n_s finds node n_d as destination. In the same way LR of relay hops also updated by their one hop level source node in route. Each node accepts LS, LD or LR given by other nodes. To prevent tampering and unethical practices such as updating thresholds of a node by its own LSU, the laurel update process opts to an LSU signature strategy. In some cases nodes may attempt to accept laurel given by the companion node is positive, otherwise discards. To avoid such practices, the proposal devised a strategy called blind update of laurel thresholds. The process of Laurel update elaborated in following sections.

2.2.1 Blind LD Update Strategy

Upon completion of the routing process between any two nodes n_s and n_d, the laurel update process will be initiated. According to the act of node n_d as destination the source node n_s updates LD of node n_d by adding LD-state. Then the updated LD of the node n_d will be signed by the node n_s. Then it will be sent to destination node n_d in encrypted format. The synchronous encryption process that devised in our earlier research article [A] is opted for encryption and decryption. Once LD accepted by the target node n_d, then it acknowledges the same to source node n_s. Then the source node sends the key to target node n_d, which will be used to decrypt the earlier received LD and maintains for further reference. The process explored in following steps. The same strategy is used even in the case of updating LS. The above said process is done at the LSU module of the responsible nodes. The process flow of LD update explored in following steps:

- Source node n_s collects the LD of the destination node and verifies the signature of the LD.
- If signature of the LD is valid and source node convinced n_d as destination by it LD value then initiates routing to n_d as destination.
- Upon completion of the routing, the source node estimates the LD-State as follows:

$$LD-State(n_s \rightarrow n_d) = 1 - \frac{1}{rt(n_d)} \quad (18)$$

Here in Eq.(18) $rt(n_d)$ indicates the retransmissions required during routing due to node n_d

- Then node n_s accumulates it to LD of the node n_d and then adds signature for authenticating the update of the LD.
- Finally sends the updated LD to node n_d in encrypted format.
- Upon receiving the LD by node n_d , it acknowledges the same with node n_s .
- Upon receiving the acknowledgement from n_d , it sends key to node n_d .
- Upon receiving key by node n_d , it decrypts the LD that received earlier in encrypted format

2.2.2 Blind LS update

The similar process that opted for updating LD by source node n_s is used to update LS of the source node n_s by destination node n_d . The LS-State will be measured as follows

$$LS-State = 1 - \frac{1}{rt(n_s)} \quad (19)$$

Here in Eq.(19), $rt(n_s)$ indicates the retransmissions required due to the tampered and inaccessible packets received by n_d .

The LS update process is quite similar to that explored for LD update.

2.2.3 Blind LR update

The similar process that opted for updating LD by source node n_s and LS by destination node n_d is used to update LR of the relay nodes $n_i.....n_{i+m}$ by their relay hop level source nodes. The LR-State will be measured as follows

$$LR-State = 1 - \frac{1}{rt(n_i)} \quad (20)$$

Here in Eq.(20), $rt(n_i)$ indicates the retransmissions required due to relay hop node n_i . The LR update of node n_i occurs at its relay hop level source node n_{i-1} .

Further process of LR update is quite similar to that explored for LD and LS update.

2.3 Route establishing

The proposed model can be build over any of the routing strategies such as AODV and DSR

The route request by source node is similar to of the base routing topology.

During the Route response, the response packets carry LR of the relay nodes along with their node ids.

During the selection of optimal route, The LR-norm will be considered. The LR-norm will be measured as follows

Find the average LR $avg_{LR}(rresp_i) = \frac{\sum_{i=1}^{R} LR_i}{R}$ (21)

Here in Eq.(21), $avg_{LR}(rresp_i)$ indicates the average LR of the relay nodes participating in the route traced by route response packet $rresp_i$ and R is total number of relay hop nodes in route traverse by $rresp_i$.

Then LR-norm will be measured as follows:

$$LR-norm(rresp_i) = 1 - \frac{1}{R'} \quad (22)$$

Her in Eq.(22), R' is number of relay hop nodes in route traversed by $rresp_i$ with LR less than $avg_{LR}(rresp_i)$

Then finally the route with less LR-norm will be selected as optimal to perform routing.

3. SIMULATION AND RESULTS EXPLORATION

The proposed model is simulated as an extension to AODV and performed extensive simulations of extremely sparse ad-hoc network with divergent network characteristics such as nodes with extremely high mobility and negligible node halt time. The simulations are mainly focused to explore the potentiality of the proposed model against black hole attacks, but elevated as this model is applicable to a broader range of attacks like grey hole.

The simulator NS2 was utilized in accomplishing the tests. Considering the mobility and node count ranging from 20 to 200, an ad hoc network simulation has been constructed. The attributes and the values of the simulation are explained in the below table 1. The main goal of this simulation is to contrast the AODV and AODV with AODV-LV.

Number of nodes Range	20 to 200
Dimensions of space	1500 m × 300 m
Nominal radio range	250 m
Source–destination pairs	20
Source data pattern (each)	4 packets/second
Application data payload size	512 bytes/packet
Total application data load range	128 to 512 kbps
Raw physical link bandwidth	2 Mbps
Initial ROUTE REQUEST timeout	2 seconds
Maximum ROUTE REQUEST timeout	40 seconds
Cache size	32 routes
Cache replacement policy	FIFO
Hash length	80 bits
certificate life time	2 sec

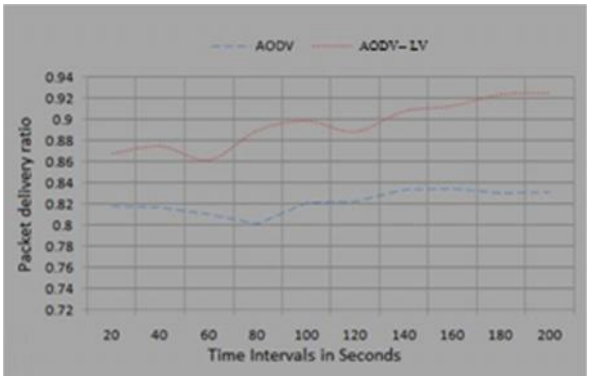
Table1: Simulation attributes.

In order to examine the working of the approached methodology, opted to metrics such as PDR, PDF, End-To-End Delay and Routing Overhead. The description of these metrics observed in simulations explored below:

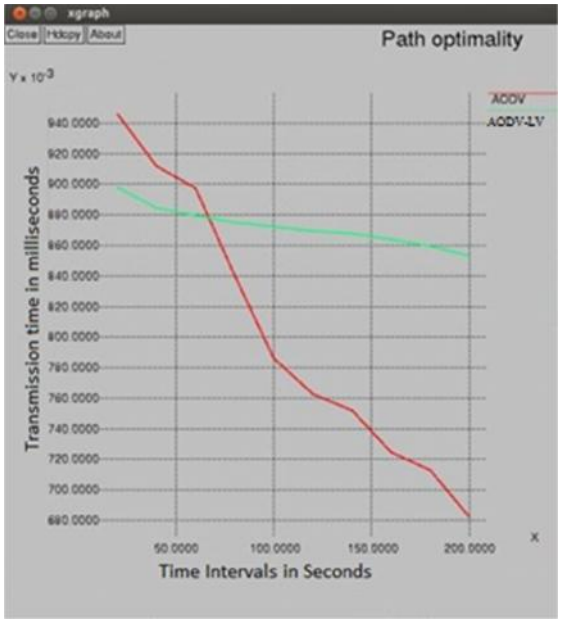
Figure (a) illustrates Packet Delivery Ratio (PDR) for AODV and AODV-LV. By considering this output it is enough to prove that AODV-LV manages maximum failure of PDR than that of AODV. Fairly accurate failure amount of PDR that is restored by the AODV-LV than AODV is 1.5%. This is balanced amount among the pauses. The least amount of restoring examined is 0.18% and the highest id 2.5%. The next Figure (b) specifies AODV benefit than that of AODV-LV in case of Path optimality in sparse number of nodes. AODV-LV utilized nearly 0.019 hops more when compared to AODV in sparse number of nodes as the reason of LR-norm confirmation method of the AODV-LV which removes the relay hop nodes that are invalid. This can be negligible in the context of fair routing achieved by AODV-LV.

Figure (c) proves that AODV-LV has less packet overhead than that of AODV. This benefit of the AODV-LV could be feasible as a reason of availability of stable routes without negotiation or irrational nodes. The Packet overhead derived in AODV is nearly 5.29% higher than packet overhead derived in AODV-LV. The slightest and uppermost packet overhead in AODV than AODV-LV derived is 3.61% and 7.29% correspondingly.

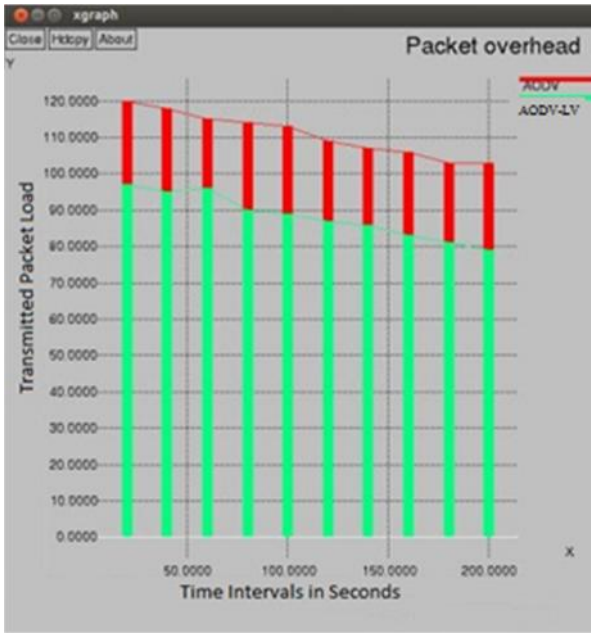
MAC load overhead is high in AODV-LV than AODV to some extent. This is viewed in figure (d). This is occurred due to the control packet swap in AODV-LV for LS, LD and LS exchange. The common MAC load overhead in AODV-LV than AODV 1.64%. The slightest and uppermost MAC load overhead derived is 0.81 and 3.24% correspondingly.



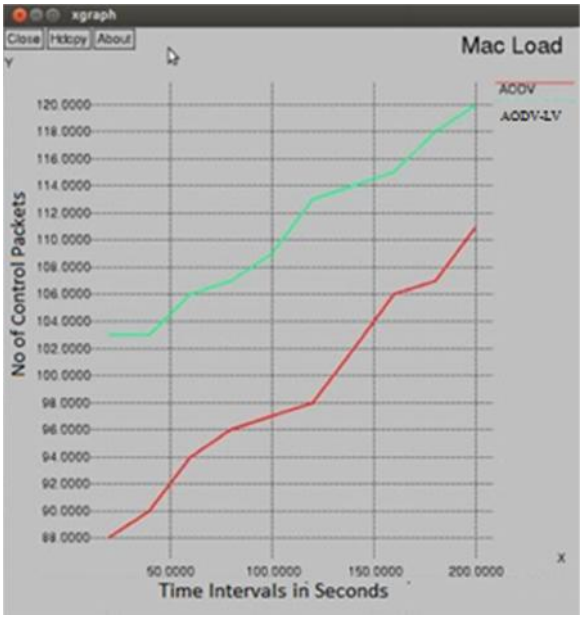
(a) Packet delivery ratio assessment



(b) Illustration for Path optimality



(c) Packet overhead assessment



(d) MAC load assessment illustrated in bar chart format

Figure: Assessment details for AODV-LV functioning than AODV

4. CONCLUSION

In this research article, a novel laurel verification strategy, which aimed to avoid the irrational and selfish nodes from the network activities. As a secure routing topology, the proposed model can be sync with any of the existing routing protocols. In experimental analysis, we adapted AODV as base routing protocol and verified the performance of the proposed Laurel verification strategy. The simulation results are indicating the scalability and optimality of the Laurel verification strategy, which compared with performance of the AODV. In future the similar laurel verification can be devised for ad hoc networks under high speed mobility.

REFERENCES

[1] K.Sreenivasulu,,E.V.Prasad and,A.Subramanyam "Performance Analysis of MANET Reactive Routing under Security" International Journal of Computer Applications (0975 – 8887) Volume 60– No.7, December 2012

[2] S. Buchegger, "Reputation Systems for Self-Organized Networks: Lessons Learned," In IEEE Technology and Society Magazine, Toward Fourth Generation Wireless, March 2008., pp. 1-10.

[3] J. Ruiz, et al, "Black Hole Attack Injection in Ad hoc Networks," DSN2008, International Conference on Dependable Systems and Networks. Anchorage, Alaska, June 24-27 2008, pp. G34-G35.
[4] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Dynamic Ad-hoc NeTworks. In Proc. of IEEE/ACM MobiHOC, 2002. IEEE.
[5] H. Yang, et al, "SCAN: Self-OrganizedNetwork-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2006, pp. 1-13.
[6] A. Dadhich, "A Distributed Cooperative Approach To Improve Detection And Removal Of Misbehaving MANET Nodes", COMSWARE, 2008, pp728 - 735
[7] P. Michiardi and R. Molva, "CORE:A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Adhoc Networks", Proc. IFIP CMS, 2002.
[8] S. Buchegger and J.L. Boudec, "A robust reputation system for peer-to-peer and mobile ad-hoc networks", proc. of P2PEcon, 2004..
[9] M.T. Schlosser, "The EigenTrust Algorithm for Reputation Management in P2P Networks," ReCALL, 2003.
[10] H. Deng, W. Li, and D. P, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol 40, 2002.
[11] U. Jian Yin, Sanjay Kumar Madria, "AHierarchical Secure Routing Protocol against Black Hole Attacks in SensorNetworks," IEEE-SUTC, vol. 1, 2006.
[12] S. Ramaswamy et al., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", ICWN'03, USA 2003..
[13] S. Ramaswamy et al, "Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks," ICWN'05, 2005, pp. 595-604.
[14] F. Li, J. Wu, and B. Raton, "Mobility Reduces Uncertainty in MANETs", Proc. of IEEE INFOCOM, May 2007.
[15] E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Source, 2007, pp. 32-40.
[16] C.E. Perkins and E.M. Royer, "Ad-hoc on-demand distance vector routing,", In proc. of 2nd IEEE Workshop on Mobile Wireless Networks, 1999.
[17] C.W. Yu, et al, Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks, Springer 2009.
[18] A. Dadhich, et al. "A Distributed Cooperative Approach To Improve Detection And Removal Of Misbehaving MANET Nodes", COMSWARE, 2008.

K.Sreenivasulu presently working as professor & HOD CSE in Madina Engineering College Kadapa.AP He is currently pursuing Ph.D from JNTUK He received B.E in Computer science from Bangalore University. He received his M.Tech in Computer Science from JNT University. He is having more than 14 years of experience in teaching. He has guided several graduate & post graduate students in their Academic projects.

Dr. E. V. Prasad received B.E. degree in ECE from S.V. University, Tirupati, A.P., India, in 1975. He obtained M.E. in Control Systems from Madras University, Madras, India, in 1978. He received his Ph.D. degree in Computer Science and Engineering, from University of Roorkee (IIT Roorkee) in 1990. He is having 36 years of teaching experience. He received best teacher award from Government of Andhra Pradesh, in the year 2008. During his teaching profession, he worked at different capacities such as Lecturer, Senior Lecturer, Assistant Professor, Professor, Head of Department of CSE, Vice Principal, Principal Director I.S.T , Registrar ,Rector of JNTUK. Currently he is working as Director Lakireddy Balireddy College of Engineerinh , Mylavaram Vijayawada A.P India. He co-authored three text books. He is life member of ISTE, IE(I), CSI, and IEEE. He has more than 102 research publications in proceedings of National, International Conferences, National and International Journals.

Dr.A.Subramanyam received his Ph.D. degree in Computer Science and Engineering from JNTU College of Engineering, Anantapur. He has obtained his B.E. from University of Madras and M.Tech from Visweswaraiah Technological University. He is having 22 years' experience in teaching. He is currently working as professor & HOD in the Department of Computer Science Engineering of Annamacharya Institute of Technology & Sciences, Rajampet, KADAPA Dist. A.P. He has presented and published number of papers in international and national conferences and number of technical paper in international and national journals. He is guiding few Ph.D.s. His research areas of interest are parallel processing, image processing, network security and data ware housing, mobile computing.