ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, No 6, June 2013

Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment

N.R.Suganya, S.Madhu Priya

Abstract— **A Mobile ad hoc network (MANET) is a peer-to-peer multihop mobile wireless network that has neither a fixed infrastructure nor a central server. In a MANET every node works as a router, and communicates with each other. The mobility constraints of mobile nodes and resource could lead to network partitioning or degradation in performance. Previously many data replication techniques have been anticipated to decrease performance degradation that is all mobile nodes work together completely in terms of sharing their memory space. These selfish nodes may possibly decrease on the whole data accessibility in the network. Because of such problem the overall process of MANET got affected. Through this problem, from the perspective of replica allocation, we observe the impact of selfish nodes in a mobile ad hoc network which is termed as selfish replica allocation. Our work was stimulated by the statement that a selfish replica allocation could lead to overall poor data accessibility in a MANET. In our enhancement proposal we tried to mitigate routing mischief by restrictive the number of packets advanced to the mischievous nodes. Trace-driven models show that our solutions are efficient and can effectively mitigate routing misbehavior. Our approach can detect two different types of routing manipulation while maintaining a low rate of false positives when show the simulation results.**

***Index Terms*—Data Replication Techniques, False Alarm Rates, Mitigating Routing Behavior, Replica allocation, Selfish Nodes, Selfish Replica Allocation.**

I. INTRODUCTION

Network partitions can arise commonly, because nodes move freely in a MANET, causing some data to be regularly unapproachable to some of the nodes. Therefore, data accessibility is frequently an important performance metric in a MANET. Data are typically simulated at nodes, other than the innovative owners, to enhance data accessibility to manage with frequent network partitions. Data replication can concurrently get better data accessibility and diminish query delay in MANET; the nodes have enough memory space to grasp both all the replicas and the unique data. A node may be active selfishly by using its limited resource only for its individual benefit, as each node in a MANET has resource limitations, for instance battery and storage restrictions. A node would like to have the profits offered by the resources of other nodes, but it may not formulate its own resource obtainable to help others. Such selfish behavior can potentially cause a wide range of problems for a MANET. They examined the impact of selfish nodes in a mobile ad hoc network from the perception of replica allocation to determine such difficulty. In scrupulous we extend a selfish node detection algorithm that believes partial selfishness and novel replica allocation methods to correctly manage with selfish replica allocation.

Different techniques have been suggested to handle the problem of selfish behavior from the network viewpoint. As expressed, the techniques handling selfish nodes can be confidential into three categories: reputation-based, credit-payment, and game theory-based methods. In reputation-based a large number of systems fit in to the first category, with varying implementations. One benefit of such methods could be their quick junction in detecting node naughtiness, particularly in a large ad hoc network, because of augmented information concerning a particular node's behavior. Though, this approach has two potential disadvantages: they frequently assume that nodes that send standing information about their peers are themselves dependable; and they are focus to collusion between nodes that misreport standing information. In credit-payment methods, every node provides a credit to others, as a reward for data forwarding. The acquired credit is then employed to forward data to other nodes. The game theory-based methods believe that all rational nodes can establish their own best possible strategies to exploit their profit. The game theory-based methods desire to discover the Nash Equilibrium direct to exploit system performance. Though this system having the drawbacks, that the standing information about their peers is themselves dependable in selfishness finding nodes. Collusion happens amongst nodes that misreport status information. Also selfish nodes might not broadcast data to others to preserve their own batteries.

We have projected a selfish node detection technique and novel replica allocation methods to feel the selfish replica allocation properly. The projected strategies are stimulated by the real-world inspections in economics in terms of credit risk and in human friendship organization in terms of choosing one's friends absolutely at one's own maturity. We functional the notion of credit risk from economics to distinguish selfish nodes. Each node in a MANET computes credit risk information on other associated nodes independently to compute the degree of selfishness. Because traditional replica allocation methods unsuccessful to believe selfish nodes, we also projected novel replica allocation techniques. First we notice the selfish node by self replica allocation. Employ those replica we formulate novel replica allocation techniques with the urbanized selfish node detection method. They are

Manuscript received May 12, 2013.

N.R.Suganya, *Pursuing M.E in Computer science Engineering, Anna University/ ASL Pauls College of Engineering and Technology ., Coimbatore, India.*

S.Madhu Priya, *Assistant Prof. Department of Computer Science, Anna University/ ASL Pauls College of Engineering and Technology/ Coimbatore, India.*

based on the perception of a self-centered friendship tree (SCF-tree) and its deviation to get high data accessibility with small communication cost in the occurrence of selfish nodes. The SCF-tree is stimulated by our human friendship organization in the real world. In the real world, a friendship, which is a form of social attachment, is complete independently. For instance, although A and B are friends, the friends of A are not always the same as the friends of B. With the help of SCFtree, we aim to reduce the communication cost, while still achieving good data accessibility. The technical contributions of this paper can be summarized as follows.

- Recognizing the selfish replica allocation difficulty: We observation a selfish node in a MANET from the viewpoint of data replication, and recognize that selfish replica allocation can lead to dishonored data convenience in a MANET.
- Detecting the fully or the partially selfish nodes efficiently: We work out a selfish node detection technique that can gauge the degree of selfishness.
- Allocating replica efficiently: We suggest a set of replica allocation methods that use the self-centered friendship tree to decrease communication cost, even as achieving excellent data accessibility.
- Proving the projected approach: The reproduction results confirm the effectiveness of our projected approach.
- Proving the projected approach: The reproduction results confirm the effectiveness of our projected approach.
- Then we suggest a method to mitigate routing misbehaviour by limiting the number of packets forwarded to the misbehaving nodes.

Behind structure the SCF-tree, a node assigns replica at each relocation period. Every node inquires non-selfish nodes within its SCF-tree to hold replica when it cannot hold replica in its local memory space. Because the SCF-tree based replica allocation is achieved in a fully distributed manner, every node decides replica allocation independently without any communication with other nodes.

II. Related Work

Frank Kargl et.al [2] spotlighted on the exposure phase and produced different kinds of sensors that can be utilized to discover selfish nodes. First they present simulation results that illustrate the negative effects which selfish nodes grounds in MANET. This mechanism explained next is called iterative probing, unambiguous probing, and activity-based overhearing. Simulation-based analysis of these mechanisms illustrates that they are highly effective and can reliably detect a multitude of selfish behaviours. This having the problem with simulations is that all the thresholds need to be set physically to facilitate getting good detection outcomes. Ioanna Stamouli et.al [3] offered RIDAN, a novel design that utilizes knowledge-based intrusion detection techniques to discover in real-time attacks that an opponent can carry out in opposition to the routing fabric of a mobile ad hoc network. Their system is planned to obtain counter measures minimising the effectiveness of an attack and maintaining the performance of the network within satisfactory limits. That RIDAN does not establish any alterations to the original routing protocol because it works as an intermediary component between the network traffic and the utilised protocol with least dispensation transparency. Takahiro Hara et.al [6] projected three replica allocation methods presumptuous that each data item is not rationalized. In these three methods, they acquired into account the access frequency from mobile hosts to each data item and the position of the network connection. Then, they expanded the proposed methods by taking into consideration is episodic revises and integrating user profiles consisting of mobile users' schedules, read/write patterns, and access behavior. Jerzy Konorski et.al [7] urbanized an approach for discovering and coping with the selfish nodes. Paper illustrates a new framework based on Dempster-Shafer theory-based selfishness detection framework (DST-SDF) with some mathematical background and simulation testing. Yet, there are still a number of obstructions to be conquered. Khairul Azmi Abu Bakar et.al [10] offered a new method to perceive those selfish nodes. Every node is established to contribute to the network on the repetitive basis within a time outline. Those which fail will endure a test for their distrustful behavior.

Jagadeesh Kumar [15] examined the crash of selfish nodes in a mobile ad hoc network from the outlook of replica allocation is observed. The selfish replica allocation could direct to decrease the overall data convenience in a MANET. A collective credit risk & collaborative watchdog process is proposed to notice the selfish node and also concern the SCF tree based replica allocation technique to handle the selfish replica allocation properly. The planned method recovers the data accessibility, decreases communication cost and average query delay, and also to diminish the detection time and to advance the accuracy of watchdogs in the collaborative approach. Manuel et.al [16] projected a collaborative approach for discovering black holes and selfish nodes in MANET.s, using a set of watchdogs which collaborate to augment their individual and collective performance. The paper demonstrates that using this collaborative watchdog advance the detection time of misbehaved nodes is reduced and the overall accuracy increased. Enrique Hern´andez-Orallo et.al [18] utilized Watchdogs are used to detect selfish nodes in computer networks. Routing misbehavior has been widely studied in mobile adhoc networks. Much work has been done to detect packet dropping and mitigate routing misbehavior. In [19] two extensions to the Dynamic Source Routing algorithm (DSR) [20] to mitigate the belongings of routing behavior are proposed: watchdog and path rater.

III. Existing Work

A. *Finding Selfish Node*

The network is represented as a set of N wireless mobile nodes with C collaborative nodes and S selfish nodes (N = C +S). At a definite period, or relocation period, every node performs the following procedures:

- Every node notices the selfish nodes based on credit risk scores (CR).

- Every node creates its own (partial) topology graph and constructs its own SCF-tree by not including selfish nodes.
- Every node allocates replica in a fully distributed manner based on SCF-tree.

The CR score is reorganized as a result at some point in the query processing phase to successfully evaluate the "degree of selfishness".

$$\text{Credit Risk} = \frac{\text{expected risk}}{\text{expected value}}$$

A node desires to recognize if another node is believable, in the intelligence that a replica can be paid back, or served upon request to divide a memory space in a MANET. By way of the considered degree of selfishness, a novel tree that symbolizes relationships among nodes in a MANET is proposed for replica allocation termed the SCF-tree. The key strength of the SCF-tree-based replica allocation methods is that it can diminish the communication cost, at the same time as achieving high data accessibility. This is since every node identifies selfishness and constructs replica allocation at its own judgment, without forming any group or engaging in lengthy negotiations.

At every repositioning period, node N_i perceives selfish nodes based on nCR^k_i. Each node might have its own initial value of P^k_i as a system parameter. The initial value of P^k_i can distinguish the essential attitude toward strangers. For illustration, if the initial value equals zero, node Ni forever pleasures a new node as a non-selfish node. As a consequence, N_i can assist with strangers easily for cooperative replica involvement. Replicas of data items are distributed by allocation techniques. After replica allocation, Ni sets ND^k_i and SS^k_i consequently. Recall that both ND^k_i and SS^k_i are approximated values, not accurate ones. The assessed values are fine-tuned at query processing time, according to given below Algorithm.

Pseudo code to detect & update sefdish features
procedure call detection()
for (each connected node N_k*){*
if$\left(nCR_i^k < \delta\right)$ N_k*is marked as non − selfish;*
else N_k *is marked as selfish;}*
wait until replica allocation is done;
for(each connected node N_k*){*
if(N_i *has allocated replica to* N_k*){*
ND_i^K = *the number of allocated replica;*
SS_i^K = *the total size of allocated replica;}*
else{
$ND_i^K = 1$;
SS_i^K = *the size of a data item;*
}}}
procedure call update_SF(){
while (during the predefined time ω*){*
if(an expected node N_k *serves the query)*
decrease P_i^K;
if (an unexpected noide N_j *serves the query){*
$ND_i^j = ND_i^j + 1$;
$SS_i^j = SS_i^j + (\text{the size of a data item})$;
if(an expected node N_k *does not serve the query){*
increase P_i^K;
$ND_i^K = ND_i^K - 1$;
$SS_i^K = SS_i^K - (\text{the size of a data item})$;
}}

IV. Proposed Work

In this chapter, we talk with routing misbehavior in DTNs as a result of responding two questions: how to perceive packet dropping and how to limit the traffic flowing to the misbehaving nodes. We first propose a scheme which detects packet dropping in a distributed manner. In this scheme, a node is required to keep previous signed contact records such as the buffered packets and the packets sent or received, and report them to the next contact node which can detect if the node has dropped packets based on the reported records. Misbehaving nodes may falsify some records to avoid being detected, but this will violate some consistency rules. To detect such inconsistency, a small part of each contact record is disseminated to some selected nodes which can collect appropriate contact records and detect the misbehaving nodes with certain probability. Then we propose a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes.

A. Routing Misbehavior Mitigation

To mitigate routing misbehavior, we try to reduce the number of packets sent to the misbehaving nodes. If a node is detected to be misreporting, it should be blacklisted and should not accept packets from others. Though, if a noncompliant node does not misreport, cannot basically blacklist it since it is dipping packets, because a usual node might furthermore drop packets because of buffer excess. In the follow, spotlight on how to mitigate routing misbehavior with no disturbing average nodes excessively a lot when disobedient nodes do not misreport. The fundamental thought is to preserve a metric forwarding probability (FP) for every node based on if the node has stopped, established and advanced packets in recent associates, which can be obtained from its accounted contact records. The nodes that repeatedly drop packets other than infrequently forward packets will have a small FP and will obtain few packets from others. Our scheme borrows ideas from congestion control to update FP. More specifically, it combines additive increase, additive decrease, and multiplicative decrease to differentiate misbehaving nodes from normal nodes.

B. Forwarding Probability Maintenance

Every node preserves an FP for each new node it has connected based on the local knowledge attained from preceding contacts, and renews the FP with new contacts. Let $\gamma(0 \le \gamma \le 1)$ indicate the FP that node N_j preserves for N_j. When N_i contacts N_j, it gets the latest contact records of N_j which are utilized to derive if N_j has dropped, established, and forwarded packets in the report window. If N_j has dropped packets, N_j reduces γ by a multiplicative factor $\rho(0 \le \rho \le 1)$. If N_j has not crashed packets, there will be two subcases. If N_j

has established packets or forwarded packets out, N_i recognizes that N_j has donated its defense or bandwidth to the network, and it enlarges γ by a preservative quantity $\delta(0 < \delta < 1)$. If N_j has not established or forwarded any packets, it can either be a disobedient node or a normal node. For defense anxieties, N_i predictably obtains as mischievous, and reduces γ by δ.

A mischievous node may "forward" packets to or "obtain" packets from its colluder by means of the out-band channel, to mislead its contacted nodes to enlarge the FP for it. To deal with this problem, node N_i keeps a measure catalog for each other node N_j it has contacted, which comprises the nodes contacted by N_j that N_i examines in the recent c contacts with N_j. If N_j repeatedly launches the above collusion behavior, its colluder will appear recurrently in the estimate list. When N_i observes that N_j has forwarded packets in the report windowN_i, confirms if the packets are forwarded to the top $r-1$ nodes which emerge most repeatedly in the estimate list. If this is accurate, it is very probable that N_j has "forwarded" packets to its plotter, and N_i will not increase the FP for N_j. Here, is the number of plotter. When r is small, we use $c = 10$. The initial value of FP is recommended to be set smaller than 1, which indicates a node from the start does not completely trust other nodes but it regularly builds the trust on them. We set the initial FP as 0.6. Newly, found out the lower which means a fast decrement, joined with a low which means a slow augmentation can result in good performances. Utilize $\rho = 0.1$ and $\delta = 0.1$.

C. *Dealing with Packet Dropping*

Assume node N_i has chosen a set of packets according to the routing algorithm to forward to its contacted node N_j. Let denote this set of packets. Then N_i forwards them, with the following strategy

$$For\ \ m \in s_{opt},\ forward\ m\ with\ probability\ \gamma$$

The proposed scheme can effectively alleviate routing misbehavior, because if a node is misbehaving and frequently drops packets, it will be assigned a low FP by its contacted nodes and obtain few packets from them. The method has the minimum (or no) result on the standard nodes that hardly ever or never drop packets. For the "hot spot" usual nodes that obtain many packets from others and habitually drop them due to buffer excess, method will decrease the amount of packets forwarded to them, and therefore alleviate the jamming at these nodes.

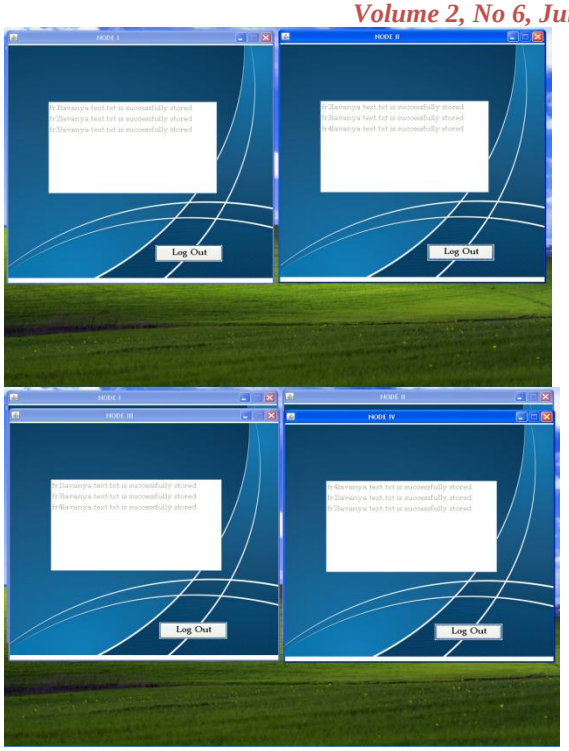


Fig (1) Data being splited for security issues

V. EXPERIMENTAL RESULTS

We analyze and compare the relocation period by average query delays. The relocation period and results of the relocation period is performed using existing and proposed method. The existing method is less performs than the proposed system. Based on the relocation period and the results from the experiment shows the proposed algorithm performs better than the other existing systems with less relocation period. Also the relocation period rate of the existing and proposed method's results is shown in the following Figure. These graph we have taken two parameters called relocation period and average query delays.

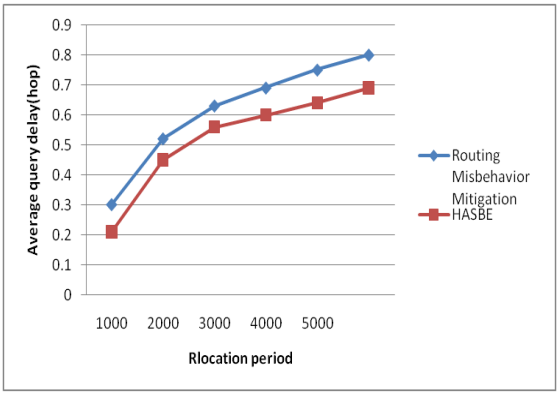


Fig (2) Query delay with varying relocation period

We analyze and compare the selfish nodes by average query delays. The selfish nodes and results of the selfish nodes are performed using existing and proposed method. The existing method is less performs than the proposed system. Based on the selfish nodes and the results from the

experiment shows the proposed algorithm performs better than the other existing systems with less selfish nodes. Also the selfish nodes rate of the existing and proposed method's results is shown in the following Figure. These graph we have taken two parameters called selfish nodes and average query delays.

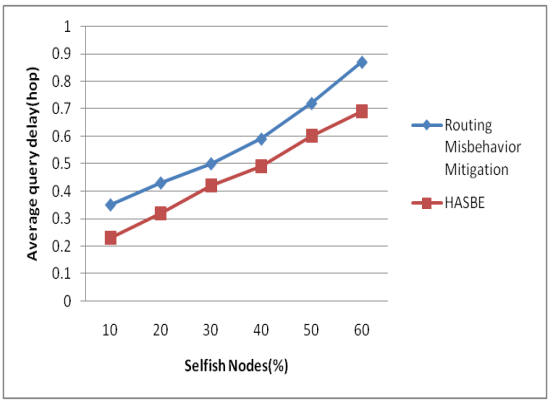


Fig (3) Query delay with varying selfish nodes

We analyze and compare the size of memory space by average query delays. The size of memory space and results of the size of memory space is performed using existing and proposed method. The existing method is less performs than the proposed system. Based on the size of memory space and the results from the experiment shows the proposed algorithm performs better than the other existing systems with less size of memory space. Also the size of memory space of the existing and proposed method's results is shown in the following Figure. These graph we have taken two parameters called size of memory space and average query delays.

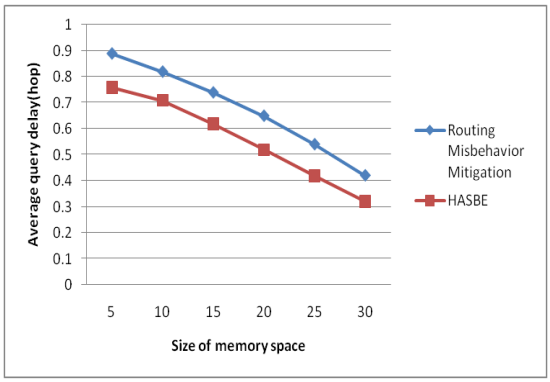
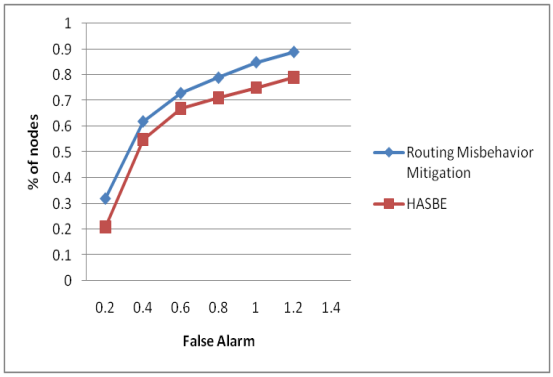


Fig (4) Query delay with varying size of memory space

We analyze and compare the false alarm rate by nodes. The false alarm rate and results of the false alarm rate is performed using existing and proposed method. The existing method is less performs than the proposed system. Based on the false alarm rate and the results from the experiment shows the proposed algorithm performs better than the other existing systems with high false alarm rate. Also the false alarm rate of the existing and proposed method's results is shown in the following Figure. These graph we have taken two parameters called false alarm rate and nodes.



Fig

(5) False alarm rate

VI. CONCLUSION

The projected selfish node detection method and novel replica allocation techniques handle the selfish replica allocation properly. In our method the each node computes credit risk information on other associated nodes individually to appraise the degree of selfishness. The Routing Misbehaviour Mitigation decreases the overall recognition time with a condensed cost in term of message overhead. This decline is very important when the watchdog detection effectiveness is low down. In addition this diminution can be attained even with a reasonable extent of collaboration. Widespread simulation results illustrates that the projected strategies outperform existing representative supportive replica allocation methods in terms of data accessibility, communication cost and query delay. We are presently working on the impact of different mobility patterns. We plan to recognize and handle false alarms in selfish replica allocation. As future work we plan to extend this model to evaluate the effect of false positives and false negatives. So an updating strategy may be needed. We also plan to evaluate the case of malicious or cheating behaviour by introducing some kind of reputation scheme.

REFERENCES

[1] Extended Report.Hugo Miranda Lu´ıs Rodrigues,"Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks", published in the IEEE International Workshop on Mobile Distributed Computing (MDC). Providence, Rhode Island USA, May 2003

[2] Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks"2004

[3] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari,"Real-time Intrusion Detection for Ad hoc Networks", Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks,2005

[4] Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney,"TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", 2005 IEEE

[5] Martin Schütte,"Detecting Selfish and Malicious Nodes in MANETs", HPI/UNIVERSITÄT POTSDAM, SOMMERSEMESTER 2006

[6] Takahiro Hara, "Data Replication for Improving Data Accessibility in Ad Hoc Networks", IEEE Transactions On Mobile Computing, Vol. 5, No. 11, November 2006

[7] Jerzy Konorski and Rafał Orlikowski, "A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks", Journal of Telecommunications and Information Technology 2009

[8] Santhosh Krishna B.V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism", International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010

[9] R. Kalaiarasi1, Getsy S. Sara2 S. Neelavathy Pari3 and D. Sridharan, "Performance Analysis Of Contention Window Cheating Misbehaviors In Mobile Ad Hoc Networks", International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010
[10] Khairul Azmi Abu Bakar and James Irvine,"Contribution Time-based Selfish Nodes Detection Scheme", ISBN: 978-1-902560-24-3 © 2010 PGNet
[11] Dipali Koshti, Supriya Kamoji, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", ISSN: 2231-2307, Volume-1, Issue-4, and September 2011
[12] S.Tamilarasan and Dr.Aramudan,"A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011
[13] Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta,"Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)", ISSN 2278- 6643) | Volume-1 Issue-2, September 2012
[14] Abhishek Gupta,Amit Saxena,"Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model", International Journal of Computer Applications (0975 – 8887) Volume 57– No.12, November 2012
[15] S.J.K. Jagadeesh Kumar ,R. Saraswathi"A Combined Credit Risk and Collaborative Watchdog Method for Detecting Selfish Node over Mobile Ad-Hoc Network", ISSN: 2277 128X Volume 2, Issue 11, November 2012
[16] Manuel D. Serrat-Olmos, Enrique Hernández-Orallo, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni, "Collaborative Watchdog to Improve the Detection Speed of Black Holes in MANETs", 2012
[17] Jim Solomon Raja.D, Immanuel John Raja.J, "A Survey on Selfishness Handling In Mobile Ad Hoc Network", ISSN 2250-2459, Volume 2, Issue 11, November 2012
[18] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni,"Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog" IEEE Communications Letters, VOL. 16, NO. 5, MAY 2012
[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, " Mitigating routing misbehavior in mobile ad hoc networks", in Proc. ACM MobiCom,2000, pp. 255-265.
[20] D. Johnson, D. A. Maltz, and Broch. "The Dynamic Source Routing Protocol for Mobile Ad Hoe Networks", Mobile Ad-hoc Network (MANET) Working Group, IETF, , October 1999.
[21] S.J.K. Jagadeesh Kumar ,R. Saraswathi"A Combined Credit Risk and Collaborative Watchdog Method for Detecting Selfish Node over Mobile Ad-Hoc Network", ISSN: 2277 128X Volume 2, Issue 11, November 2012
[22] Manuel D. Serrat-Olmos, Enrique Hernández-Orallo, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni, "Collaborative Watchdog to Improve the Detection Speed of Black Holes in MANETs", 2012
[23] Jim Solomon Raja.D, Immanuel John Raja.J, "A Survey on Selfishness Handling In Mobile Ad Hoc Network", ISSN 2250-2459, Volume 2, Issue 11, November 2012
[24] Extended Report.Hugo Miranda Lu´ıs Rodrigues,"Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks", published in the IEEE International Workshop on Mobile Distributed Computing (MDC). Providence, Rhode Island USA, May 2003
[25] Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks"2004
[26] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari,"Real-time Intrusion Detection for Ad hoc Networks", Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks,2005
[27] Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney,"TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", 2005 IEEE
[28] Martin Schütte,"Detecting Selfish and Malicious Nodes in MANETs", HPI/UNIVERSITÄT POTSDAM, SOMMERSEMESTER 2006
[29] Takahiro Hara, "Data Replication for Improving Data Accessibility in Ad Hoc Networks", IEEE Transactions On Mobile Computing, Vol. 5, No. 11, November 2006
[30] Jerzy Konorski and Rafał Orlikowski, "A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks", Journal of Telecommunications and Information Technology 2009
[31] Santhosh Krishna B.V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism", International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010
[32] R. Kalaiarasi1, Getsy S. Sara2 S. Neelavathy Pari3 and D. Sridharan, "Performance Analysis Of Contention Window Cheating Misbehaviors In Mobile Ad Hoc Networks", International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010
[33] Khairul Azmi Abu Bakar and James Irvine,"Contribution Time-based Selfish Nodes Detection Scheme", ISBN: 978-1-902560-24-3 © 2010 PGNet
[34] Dipali Koshti, Supriya Kamoji, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", ISSN: 2231-2307, Volume-1, Issue-4, and September 2011
[35] S.Tamilarasan and Dr.Aramudan,"A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011
[36] Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta,"Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)", ISSN 2278- 6643) | Volume-1 Issue-2, September 2012
[37] Abhishek Gupta,Amit Saxena,"Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model", International Journal of Computer Applications (0975 – 8887) Volume 57– No.12, November 2012

N.R.Suganya is pursuing M.E in computer science and Engineering, completed MCA from Anna University, Coimbatore. Published 5 international journals based on Software testing, Networking and Digital image processing. Research work is deeply done with software testing.