A Trust And Energy-Based Efficient Routing Scheme Using Kuder-Richardson Reliability Coefficient For Manets

V.Vijayagopal, Dr. K.Prabu

Abstract : The dissemination of data between the source and destination highly relies on the trustworthy intermediate nodes. But, the presence of root node attackers degrades the network performance and increases the network overhead. Hence, the need arises for innovating trust based reputation mechanisms that could be incorporated in different routing protocols and which could effectively and efficiently mitigate black hole attacks. In this paper, Kuder-Richardson Reliability Factor based Mitigation Mechanism (KRRFMM) are proposed for mitigating rendezvous point misbehavior of core group leader. This proposed KRRFMM algorithm is identified to be excellent compared to existing CARFMM, CONFIDANT, RTBD and PCMA schemes

Index Terms: KRRFMM, CARFMM, CONTIDANT, RTBD, PCMA.

1 INTRODUCTION

A mobile ad-hoc network [1] is defined as the collection of autonomous mobile nodes that coordinates with each other for dissemination of data without any fixed infrastructure. Hence, the topology of MANETs posses a dynamic topology and the mobile nodes change its behavior drastically and the nodes at any point of time may easily join or leave the network [2]. This dynamic nature of nodes imposes a number of attacks and may degrade the performance of the entire network [3]. To accomplish effective communication several protocols such as AODV (Ad-hoc On-Demand Distance Vector), and DSDV (Destination-Sequenced Distance-Vector) and so on could be utilized. Since, the mobile ad hoc networks lacks a centralized authority, any proposed solution for enabling effective cooperation between the nodes assumes that all nodes has to be trustworthy [4]. However, in case of a hostile environment, the illegitimate nodes present in between the source and destination may launch routing attacks in order to disrupt the routing operations and may even the reliable services to cooperative nodes [5]. The black hole attack is a kind of routing attack, in which the node counterfeits with the reply saying that it has the freshest and shortest path to the destination node and at the same time absorbs all the data packets forwarded to the destination [6]. Hence, the performance of the entire network decreases. In this paper, we mainly focus on the trust based reputation mechanisms proposed for mitigating black hole attacks in MANET.

2 RELATED WORK

A competent mechanism was proposed by Satoshi Kurosawa et al [6], utilizes the training data for detecting and mitigating black hole attack which gets updated at regular interval of time. In this scheme, the detection is based on multidimensional feature vector called mean vector, which incorporates the number of RREQ messages sent and the number of RREQ received through which average difference in the destination sequence number with in the time slot of RREP is evaluated. A statistical analysis of multipath technique proposed by Lijun Quian et al [7], detects the black hole attack based on the statistics derived from the relative frequency provided by each set of the routes. Two another mitigation mechanisms namely LITEWORP and MOBIWORP [8] was proposed by Khalil S.Baghi and Shroff.N.B, possess a component called guard node which monitors all the traffic lines and detects the black hole attack. In LITEWORP, the detection is based the trusted central authority, which collects information about the neighbors that exists in two hop distance. Whereas, in MOBIWORP possess the capacity of overhearing. Latha Tamilselvan and V.Sankaranarayan et al [9] contributed a mechanism for black hole detection based on the 'timer expired table' which is first set when the RREQ is initially received by the destination node. The timer expired table contains node's sequence number, time of arrival of packets and outbound time of RREQs. This mechanism confirms the mitigation of black hole node when the redundancy of selected routes does not occur in the routing table. Yet, Shishir K.Shandilya and SunitaSahu [10] proposed a trust based solution based on the trust worthiness factor computed for each and every node. This technique calculates the trust value of the path based on the modified fields of the trust table updated in the routing table. The trust value computed lies between -1 and 1.if the value of trust lies between 0 and 1, then the node is trustworthy else the node is detected as black hole. A shared hop node based solution was proposed by Michele Nogueira Lima et al [11]., in which the sender nodes verifies the authenticity of the node that originates the RREP packets by making use of network redundancy. Since, the packets that arrive at the destination nodes may have redundant paths, the detection is based on the safe route identified by the source nodes. Yet another, N.Balaji and A.Shanmugam [12] proposed a scheme that selects the best and secured route in the ad hoc network. Each and every mobile node computes the value of the trust. This trust value computed is adjusted based on the experiences

- [1]*Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India. Ph: 8667744293, Email: vijayagopal1976@gmail.com*
- [2]*Associate Professor, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India, Ph: 9843916940, Email: kprabu.phd@gmail.com*

that it has with their neighbor nodes and the association among the individual nodes with the neighboring nodes can be categorized into Unknown nodes, Known nodes and Companion nodes.

3 The proposed Reliable Energy and Trust-based Kuder-Richardson Reliability Factor-based Mitigation Mechanism (KRRFMM) for Efficient Routing Process.

KRRFMM is a vital statistical reliability factor-based mitigation mechanism proposed for mitigating rendezvous point misbehavior from an ad hoc environment. In KRRFMM , the mitigation of rendezvous point misbehavior is facilitated using two steps that include a) Estimation of mean packet deviation, b) Calculation of variance and standard deviation for computing KRRF and c) Detection and isolation of rendezvous point misbehavior using computed KRRF.

a) Estimation of mean packet drop

Similar to CARFMM, let us consider an ad hoc network in which the mobile nodes are monitored by their neighbouring nodes for entire 's' sessions. If the number of packets forwarded and received by each node 'i' is $PF_{(1)}, PF_{(2)}, ..., PF_{(s)}$ and $PR_{(1)}, PR_{(2)}, ..., PR_{(s)}$ respectively as monitored by each of its neighbours in 's' sessions.

The number of packets dropped by each mobile node as monitored by their neighbours in each session 'c' is

$$DROP_{PACKET(c)} = PR_{(c)} - PF_{(c)} \quad (1)$$

Further, the mean packet drop of each mobile node in each session 'c' as identified by their neighbour is

$$MDROP_{PACKET(c)} = \sum_{c=1}^{s} \frac{DROP_{PACKET(c)}}{s} \quad (2)$$

b) Calculation of total variance for computing KRRF

When the value of $PR_{(c)}$ and $MDROP_{PACKET(c)}$ are computed, total variance experienced by each mobile nodes towards data packet dissemination is calculated using

$$\text{T-}VAR_{DETECT} = \sum_{c=1}^{s} \frac{(PR_{(c)} - MDROP_{PACKET(c)})}{s} \quad (3)$$

The KRRF computed based on (2) and (3) is

$$(KRRF)_{DETECT} = \frac{s}{s-1}\left(1 - \frac{\sum_{c=1}^{s}(DROP_{PACKET(c)} * PR_{(c)})}{T - VAR_{DETECT}}\right) \quad (4)$$

c) Detection and isolation of rendezvous point misbehaviour using computed CARF

When KRRF is identified for each mobile node, the decision pertaining to the detection of isolation of rendezvous point misbehaviour is initiated. The mobile nodes identified with CARF value less than 0.30 (obtained from simulation) are detected as rendezvous point misbehaviour comprimized and are isolated from the multicasting activity.

Algorithm: Kuder-Richardson Reliability Factor based rendezvous point misbehavior detection and isolation

1. Consider N number of nodes in the network.
2. The source and destination nodes are designated as SN and DN from the complete number of mobile nodes GN, representing the starting and end point of the routing path.
3. The RREQ route request packet is forwarded for establishing the routing path between SN and DN nodes.
4. The DN nodes send the acknowledgement for data transmission for initiating the SN.
5. The steps of the algorithm (6 -13) is iterated for each and every individual mobile node, 'u' that corresponds to the group of nodes GN under the time of data transmission 't'. .
6. For every node 'u'of GN in the routing path.
7. Estimate the dropped packets that quantify the difference between the number of packets received to the number of packet forwarded by each mobile node through $DROP_{PACKET(c)} = PR_{(c)} - PF_{(c)}$
8. Compute the mean packet drop of each mobile node in each session 'c' as
$$MDROP_{PACKET(c)} = \sum_{c=1}^{s} \frac{DROP_{PACKET(c)}}{s}$$
9. Calculate the total variance for computing KRRF based on the value of $PR_{(c)}$ and $MDROP_{PACKET(c)}$ using
$$\text{T-}VAR_{DETECT} = \sum_{c=1}^{s} \frac{(PR_{(c)} - MDROP_{PACKET(c)})}{s}$$
10. Determine KRRF using
$$(KRRF)_{DETECT} = \frac{s}{s-1}\left(1 - \frac{\sum_{c=1}^{s}(DROP_{PACKET(c)} * PR_{(c)})}{T - VAR_{DETECT}}\right)$$
11. If the value of KRRF associated with each node 'u' is less that 0.30, then
12. Th malicious node u is identified as a root node attacker and isolation of it from the path is initiated.
13. The procedure of Isolation of Root Node Attacker is applied.
14. Else
15. The node is estimated as trustworthy.
16. End if.
17. End for.

4 SIMULATION RESULTS AND EXPERIMENTAL

ANALYSIS

The simulation experiments of the proposed KRRFMM are conducted using ns-2.26 simulator for comparing its superiority in the network performance compared to CARFMM, CONFIDANT, RTBD and PCMA schemes. This evaluation is achieved based on a PDR, throughput, control overhead, total overhead, delay and energy consumptions with different number of mobile nodes and root node attacker nodes. This simulation experiment is deployed in a network with 100 nodes randomly placed in the network area of 1000 x 1000 meters. The simulation run is initiated for 300 seconds with 2 Mbps and 250 meters of data rate and radio range.

Results and Discussions

Initially, the proposed KRRFMM is investigated with the existing past proposed approaches like CARFMM, CONFIDANT, RTBD and PCMA for identifying the mitigation point at which rendezvous point misbehavior of nodes can be effectively handled. From the simulation result, is inferred that KRRFMM exhibits an effective performance in 0.40 since maximum numbers of rendezvous point misbehavior are detected by KRRFMM at this point than CARFMM, CONFIDANT, RTBD and PCMA considered for study. Hence, the mitigation point for detecting rendezvous point misbehavior of nodes is considered to be 0.30 for comparative study. It is also inferred that KRRFMM is also equivalently capable of identifying the maximum number of Rendezvous point misbehavior within the detection range of 0.25 and 0.35. Hence, maximum and minimum detection threshold detection point of KRRFMM is considered as 0.25 and 0.35 respectively. Further, the performance of KRRFMM is evaluated using four experiments by varying the a) number of mobile nodes, b) number of rendezvous point misbehavior, c) number of mobile nodes with maximum detection threshold point of 0.25 and d) number of mobile nodes with minimum detection threshold point of 0.35In the first part of the investigation, the potential of the proposed KRRFMM and the compared CARFMM, CONFIDANT, RTBD and PCMA are compared with different number of mobile nodes with the detection limit of 0.4. Figure 1 and 2 presents the plots of PDR and throughput evaluated for the proposed KRRFMM with different mobile nodes. The PDR is considered to get sustained in the network under the implementation of the proposed KRRFMM scheme, since the maximum degree of energy consumptions is maintained with better preservation of energy. The proposed KRRFMM resolves the issue of root node attack for improving the network performance. The proposed KRRFMM increase PDR by 9.20%, 10.65%, 12.32% and 15.69%, predominant to CARFMM, CONFIDANT, RTBD and PCMA. The proposed KRRFMM also sustains the throughput by 8.21%, 10.92%, 14.32% and 17.12%, predominant to CARFMM, CONFIDANT, RTBD and PCMA.

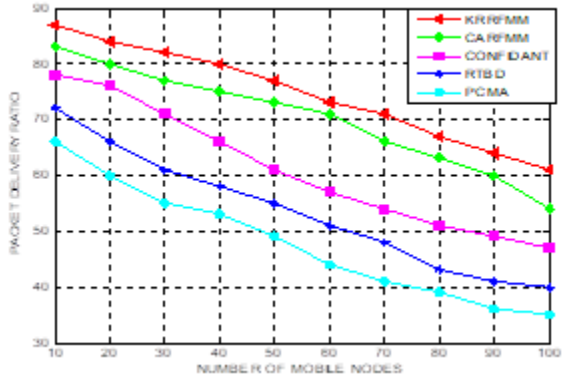

***Figure 1**-KRRFMM-Experiment 1-Packet Delivery Ratio*

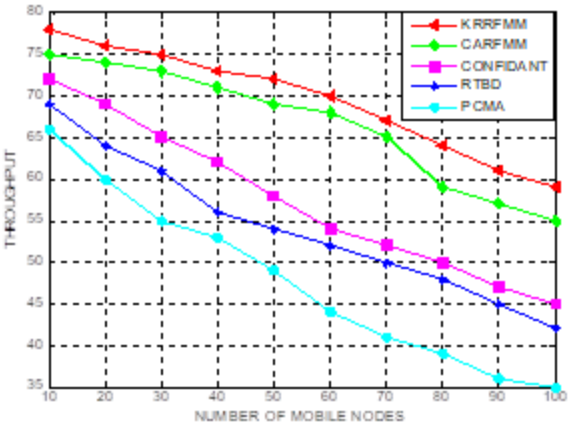

***Figure 2**-KRRFMM-Experiment 1-Throughput*

Hence, KRRFMM shows an improvement in PDR by 3%-5% over CARFMM, 6%-7% over CONFIDANT,8%-10% over RTBD and 14%-16% over PCMA. Similarly, KRRFMM improves the throughput by by 2%-3% over CARFMM, 4%-6% over CONFIDANT, 8%-10% over RTBD and 15%-17% over PCMA. In addition, KRRFMM on an average shows a phenomenal improvement of 12% and 10% in terms of PDR and throughput. Further, total overhead and control overhead of the network proportionally increases with increased number of transmissions. However, KRRFMM minimizes the control overhead by by 6%-8% over CARFNN, 10%-13% over CONFIDANT, 14%-16% over RTBD and 22%-25% over PCMA by enforcing rendezvous point misbehaviour mitigation at a rapid rate of 30% as depicted in Figures 3 and 4.

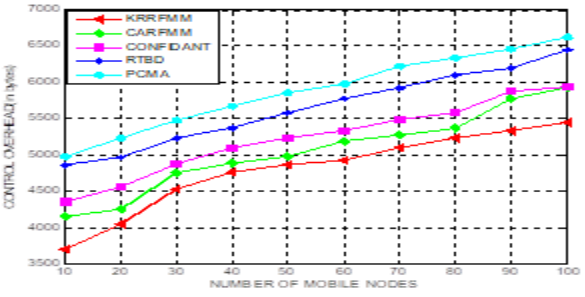

***Figure 3**-KRRFMM-Experiment 1-Control Overhead*

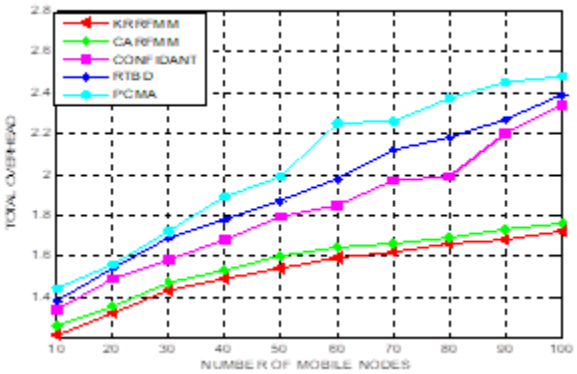

***Figure 4**-KRRFMM-Experiment 1-Total Overhead*

It is also identified that the proposed KRRFMM minimized the total overhead by by 6.58%, 11.28%, 16.84% and 22.12%, predominant to CARFMM, CONFIDANT, RTBD and PCMIn the second part of the investigation, the potential of the proposed KRRFMM and the compared CARFMM, CONFIDANT, RTBD and PCMA are compared with different number of root node attackers changed from 10 to 50. The plots of PDR evaluated for the proposed KRRFMM with different root node attackers are presented using Figure5. The PDR is considered to get sustained in the network under the implementation of the proposed KRRFMM scheme, since the maximum degree of energy consumptions is maintained with better preservation of energy. The proposed KRRFMM resolves the issue of root node attack for improving the network performance. The proposed KRRFMM increase PDR by 7.42%, 9.96%, 16.21% and 21.82%, predominant to CARFMM, CONFIDANT, RTBD and PCMA.

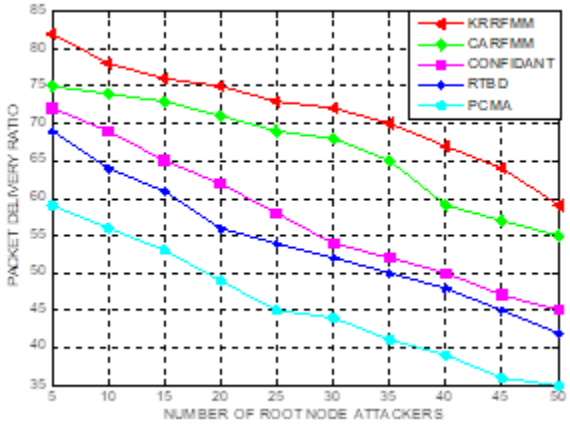

***Figure 5**-KRRFMM-Experiment 2-Packet Delivery Ratio*

Figures 6 and 7 highlights the control overhead and network delay determined with different number of rendezvous point attacker nodes in the network. It is identified that the control overhead and network delay increases with respective increase in the number of root nod attacks, since energy consumptions incurred by the malicious node greatly influences the path stability of the network. The proposed KRRFMM reduced the control overhead by 8.21%, 11.73%, 15.82% and 19.12%,predominant to CARFMM, CONFIDANT, RTBD and PCMA. The proposed KRRFMM reduced the network delay by 6.92%, 10.92%, 16.21% and 20.18%,predominant to CARFMM, CONFIDANT, RTBD and PCMA. It is also determined that the control overhead and network delay, on an average are minimized by 12.12%, and 14.58% compared to the baseline schemes.

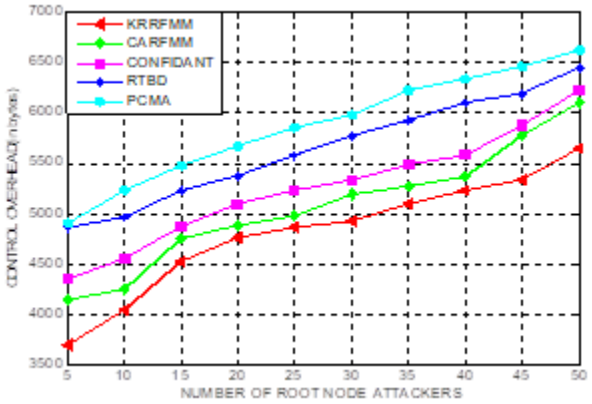

***Figure 6**-KRRFMM-Experiment 2-Control Overhead*

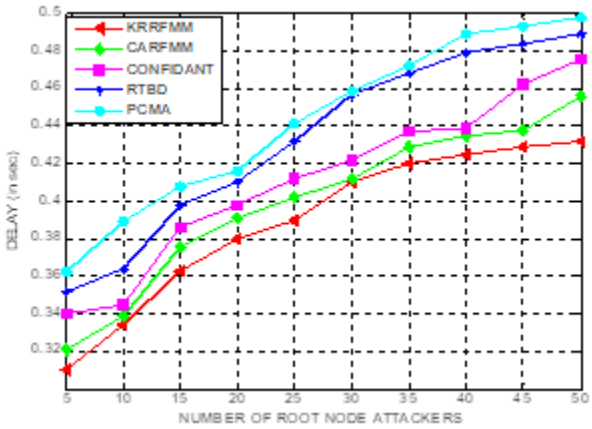

***Figure 7**-KRRFMM-Experiment 2-Delay*

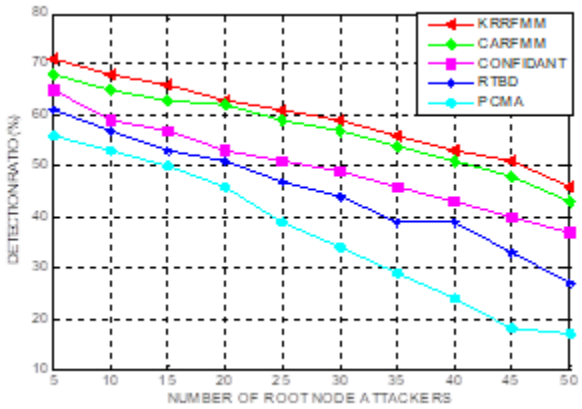

***Figure 8**-KRRFMM-Experiment 2-Detection Ratio*

In addition, the results of the proposed KRRFMM evaluated using detection rate with different root node attackers is presented in Figure 8. It is estimated that the detection rate facilitated by the proposed KRRFMM is dynamically improved to respective increase in the root node attackers. The proposed KRRFMM improved the detection rate by 8.18%, 10.12%, 13.26% and 19.12%,predominant to

CARFMM, CONFIDANT, RTBD and PCMA.

5. CONCLUSIONS

In this paper, Kuder-Richardson Reliability Factor based Mitigation Mechanism (KRRFMM) are proposed for mitigating root node attacker. The experimental results of KRRFMM outperform the proposed past history based mitigation approaches. Further, KRRFMM aids in framing a detection limit for visualizing the influence provided by the root ode attackers. Rendezvous point misbehaviour of mobile nodes can also be investigated based on energy related parameters pertaining to the role of group leader under multicasting and bayesian probability can also be used for analysing the behaviour based on past and current experience into account.

REFERENCES

[1] Bose, S., Bharathimurugan, S. and A. Kannan, Multi-layer integrated anomalyintrusion detection system for mobile adhoc networks. Proceeding of theInternational Conference on Signal Processing, Communications and Networking, pp: 360-365, 2007.

[2] Paramasiva, B. and K.M. Pitchai, Modeling intrusion detection in mobile adhoc networks as a non cooperative game. Proceeding of the InternationalConference on Pattern Recognition, Informatics and Mobile Engineering(PRIME), pp: 300-306, 2013.

[3] Marchang, N. and R. Tripathi, A game theoretical approach for efficientdeployment of intrusion detection system in mobile ad hoc networks.Proceedings of the International Conference on Advanced Computing andCommunications. Assam, pp. 460-464, , 2007.

[4] T. Anantvalee and J. Wu,. A Survey on Intrusion Detection in Mobile Ad HocNetworks, Wireless Network Security, Xiao, Y., X. Shen and D.Z. Du (Eds.) Springer, New York, pp. 159-180, 2007.

[5] Y. Hu, A. Perrig and D.B. Johnson, SEAD: Secure Efficient Distance VectorRouting for Mobile Ad Hoc Networks. Proceedings of the 4th IEEE Workshopon Mobile Com-puting Systems and Applications (WMCSA 2002),IEEE,Calicoon, NY. June 2002.

[6] Y. Hu, A. Perrig and D.B. Johnson, Ariadne: A Secure On-Demand RoutingProtocol for Ad Hoc Networks. Proceedings of the Eighth Annual InternationalConference on Mobile Computing and Networking (Mobicom 2002), pp. 12-23,ACM, Atlanta, GA, September 2002.

[7] Razak, S. A., Furnell, S., Clarke, N., & Brooke, P. (2006, May). A two-tierintrusion detection system for mobile ad hoc networks–a friend approach.Procceding of the International Conference on Intelligence and SecurityInformatics pp. 590-595, Springer, Berlin, Heidelberg.

[8] Razak, S. A, Two-tier Intrusion Detection System for Mobile Ad HocNetworks, 2007.

[9] Perkins, C., Belding-Royer, E., and Das, S., Ad hoc on-demand distance vector(AODV) routing (No. RFC 3561), 2003.

[10] Trivedi, A. K., Arora, R., Kapoor, R., Sanyal, S., and Sanyal, S. A semidistributedreputation based intrusion detection system for mobile adhocnetworks, Journal of Information Assurance and Security (JIAS), vol. 1, issue 4,pp. 265-274, 2006.

[11] Trivedi, A. K., Kapoor, R., Arora, R., Sanyal, S., &Sanyal, S. RISMReputationBased Intrusion Detection System for Mobile Ad hoc Networks,arXiv preprint arXiv:1307.7833, 2013.

[12] Thakur, M. R., and Sanyal, S, A multi-dimensional approach towards intrusiondetection system. arXiv preprint arXiv:1205.2340, 2012.

[13] Mitrokotsa, A., and Dimitrakakis, C., Intrusion detection in MANET usingclassification algorithms: The effects of cost and model selection, Journal of AdHoc Networks, 11(1), pp. 226-237, 2013.

[14] Anantvalee, T., & Wu, J., A survey on intrusion detection in mobile ad hocnetworks. In Wireless Network Security, pp. 159-180, Springer, Boston, MA, 2007.

[15] S. Bansal and M. Baker. Observation-based cooperation enforcement in adhoc networks.Technical report 072003, Stanford University, 2007.