Kuder-Richardson Coefficient Based Trust Mechanism for Service Discovery in MANETs

S. Pariselvam [#1] AND R.M.S Parvathi [#2]

[#1] Associate Professor (Research Scholar, Anna University), Department of CSE
Manakula Vinayagar Institute of Technology, Madagadipet, Pondycherry, India.
s.pariselvam@gmail.com

[#2] Professor and Principal, Department of CSE, Sengundhar College of Engineering,
Kosavampalayam,Tiruchengode,Namakkal Dt,Tamilnad,India

***Abstract*— Service discovery in Mobile Ad hoc networks is highly crucial due to the lack of centralized infrastructure. Furthermore, varieties of services available through the network may require different levels of security. Thus, a need arises for formulating and deploying an efficient trust oriented service discovery mechanism distributed in each and every node in the ad hoc scenario in order to reduce the complexity in providing the services to the network users. In this paper, we have proposed a Kuder-Richardson co-efficient based trust mechanism (KRCBM) for service discovery in MANET. This effective mechanism works with the aid of the trust value called Kuder-Richardson co-efficient, which manipulates the reliability of the group of nodes participating in the ad hoc environment. This trust model possesses an inherent ability of designating various protection levels for services discovery. Based on the designated level of the services, secure communication is established. The performances of KRCBM are analyzed through ns-2 simulations with the help of performance metrics like packet delivery ratio, Control Overhead and total overhead. From the simulation results obtained, it is proved that the proposed mechanism performs well when compared to the other trust based mechanisms available in the literature by reducing the packet drops to a maximum extent.**

Keyword - KRCBM, MANET, AODV, RREQ, RREP, RRER

1. INTRODUCTION

Service Discovery requires higher degree of co-ordination providing co-operation among the mobile nodes in a MANET is a critical issue that is not explored by most of the researchers in the past decade [1]. This is due to the lack of central infrastructure and dynamic nature of the ad hoc network. If the nodes in an ad hoc environment deny cooperating, then the network performance degrades [2]. Hence, there is need for devising reliability coefficients based algorithm for detecting and preventing the selfish nodes or the non-cooperating nodes.

From the existing literature, it is apparent that the reliability coefficients could analyze any kind of statistical data more accurately and precisely when compared to the other reliability based consistency check mechanisms available [13]. Generally, there are three categorical methods for proving reliability based consistent checks to the nodes existing in the network. They are Cornbach alpha, Correlation Coefficient and Regression coefficient.

In this proposed schema, we employ trust based reliability coefficient named Kuder-Richardson co-efficient based trust mechanism for testing the consistency in the behavior of the mobile nodes in MANETs. Here, the protocol used for carrying out is analysis is the tree based and reactive protocol called AODV. This protocol makes use of control packets like RREQs, RREPs, and RRERs for establishing the forward as reverse routes for relaying the packets.

The remaining part of the paper is organized as follows. In section 2, we enumerate some of the works present in the literature with the other possible types of coefficients that could be utilized for manipulating the node consistency levels with a brief extract of the survey. The detailed explanation of the proposed trust mechanism KRCBM is depicted in section 3.The algorithm of the proposed Trust mechanism using KRC implemented for service discovery is presented in section 4. The experimental analysis and the Simulations results are presented in section 5 and 6.Section 7 concludes the paper.

Security Issues of Service Discovery in MANETs

Some of the security issues that have to be considered in case of service oriented approach for secure communication. They are as enumerated as below:

- The presence of a single malicious node may degrade the performance of the network in a dynamic service provider's environment [1].

- The lack of centralized access point in ad hoc networks imposes a number of weaknesses for the system security designers since there are no trusted intermediateries.[2]
- MANET are prone to a number of challenges for providing security solutions due to their wide availability of resources, severe resource constraints, unclear line of defense, shared wireless medium, dynamic network topology and wireless shared medium. [3]

2. Related work

From the recent past, a lot of research has been carried out intensively for the formulation of trust based algorithms for facilitating the nodes to offer services to their users of the ad hoc networks. The mechanism present in the literature can be broadly categorized into first hand based trust mechanism and second hand based trust mechanism. Some of the solutions for facilitating high degree of inability for service discovery are enumerated below.

Alessandro Mei and Juliana Stefan, [3] contributed a multilevel trust based mechanism which makes use of force faithful behavior. This could enhance the network performance by reducing the number of duplicate thus saving the storage requirements. The author has also proposed this trust based mechanism based on the assumption that the two protocols used for their study are strategy proven and not even a single node has the interest to deviate from their normal behavior.

Stephan Eidenbenz et al,[4] proposed a distributed algorithm, which has been formulated mainly based on the four important properties like the rationality of the nodes in routing, the truthfulness of the nodes participating in the routing , Relaying the packets on the most energy efficient path and last but not the least the message has to be transmitted with less complexity. They also proposed a VCG payment scheme combined with the game theoretic technique to achieve the reliability of the node in the entire network.

Tamer Rafael et al.[5] contributed a reputation mechanism, which is deployed omnipresent in all the nodes present in an ad hoc network. In this mechanism, the node makes use of two entities namely reputation index and a reputation table. Reputation index of a node utilized in this mechanism may be defined as a monotonically increasing value computed with respect to the successful delivery of packets to its neighbors. The reputation table in turn stores the updated reputation index at each and every time session of communication. The authors have also proposed this mechanism based on three heuristic approaches namely Hops away from source, double decrement/single increment ratio and random early probation.

Ze Li and Haiying Shen, [6] proposed a trust oriented service discovery mechanism that is based on a reputation threshold parameter that could distinguish the nodes into two broad categories namely trustworthy and untrustworthy. It also proposes a virtual cash mechanism for controlling the packet servicing activity of a node. The proposed mechanism is formulated in keeping the concepts of game theory in mind. It also investigates on the cooperation of the nodes in the ad hoc network. It was also been devised as an integrated approach for dealing with service discovery in the presence of malicious nodes.

Feng Li et al, [7] proposed a trust mechanism which is also based on game theory. This mechanism was designed in order to increase the interaction among the wireless mobile nodes in MANETs. They also contributed the mechanism by considering the modeling scenario as dynamic. The authors also used Bayesian signaling game for discriminating the behavior when the normal nodes updates their strategy based on the malicious node whereas the malicious nodes always has an eye on determining strategy that could help to escape from the network. These mechanisms also possess the concept of sequential rationality and random property.

Shukor et al, [8] enumerated a mechanism that increases the degree of collaboration between the nodes while considering the availability of their stringent resources present in the scenario. They also formulated a friendship mechanism that reduces the number of false positives that occur due to presence of malicious nodes during communication for service discovery. They utilized two methodologies namely direct and indirect reputation. Their work has mainly based on the six degree of separation that could arise between the nodes in the network and how to cope with this kind of separation. They also used a voting strategy for discriminating genuine nodes from non-Genuine nodes present in an ad hoc network.

Hazer Inaltekin and Stephen B.Wicker [9] listed variety of issues that could disturb the co-ordination between the nodes in an ad hoc scenario. They formulated a game based theoretic solution based on Lévesque measure that could assign an advanced probability value to all the participating nodes in the network. They also analyzed the behavior of the network based on Nash Equilibrium function, which is manipulated based on the cost of failed transmission.

A) Types of Reliability coefficient available in the literature for checking the Trustworthiness of a node

A numerous reliability coefficients are available in statistical theory for performing a consistency check for the behavior of a participating in the network. Brief enumerations of some of the coefficients for predicting the reliability are depicted below.

1) Cornbach Alpha Coefficient [10]: This reliable consistency check coefficients are highly applicable in a scenario, where the behavior of the nodes are monitored mainly with respect to the binary outcomes or large scale data. This reliability coefficient predicts the trustworthiness of the nodes accurately rather than providing an assumption value for the reliability of the nodes.

2) Correlation Coefficient [11]: This Reliability coefficients are mainly suited in a scenario, where the behavior of the node are monitored based on the similarity of the events that could occur in a session. This coefficient provides a higher degree of accuracy when compared to the Cornbach Alpha Coefficient

3) Regression coefficient [12]: This coefficient computation provides the degree of dissimilarity between the incoming numbers of packets to the number of outgoing number of packets. Higher the regression value infers the presence of untrustworthy nodes present in a service oriented communication

B) Extract of the Literature.

The literature review carried out for identifying the presence of untrustworthy nodes present in a routing path during a service oriented communication has the following shortcomings they are:

- A trust mechanism that efficiently uses multilevel threshold values for detecting malicious nodes in a service oriented communication based on the severity or intensity of the application where service discovery becomes vital.
- A mechanism which could predict a node's maliciousness based on reliability factor at a faster rate during service discovery has not been proposed to the best of my knowledge.
- A Mechanism which could predict the presence of un trusted node based on the correctional factor has not been available in the literature.

These are the factors that motivated for devising a trust based mechanism that helps in enhancing the process of service discovery by isolating the untrustworthy nodes during routing.

3. PROPOSED SOLUTION

3.1 Overview

In this paper, we propose a Kuder-Richardson co-efficient aided trust based security mechanism for establishing service discovery in MANET in the presence of compromised nodes. The proposed trust based scheme uses the KRC as the confidence or trust factor for each and every node based on the level of its interaction and behavior in the network**.** Depending on the sensitivity of the services, the services can be classified into two namely secure services and non-secure services**.** For every level of security provided to the services , nodes computes the trust value and disseminate them to all the nodes present in the topology. The KRC trust value is always updated periodically to offer high efficient and effective trust for the service discovery model. Further, a methodology for establishing a secure communication channel is also been proposed. This mechanism utilizes the parameter of the offline authority in order to distribute nodes with trust factors. Thus, the mechanism offers trust based security to service discovery in MANET and guarantees both reliability and security at hand.

3.2 Kuder-Richardson co-efficient based trust mechanism (KRCBM) for service discovery in MANET

The proposed KRCBM trust model distributed computes the trust value based on Kuder-Richardson co-efficient (KRC) for each and every node in the network based on the context of the service provider or service requester. The KRCBM mechanism classifies the genuinety of the nodes based on four thresholds.

The Trust level (CV) among each and every node mainly relies upon the following three properties namely Reflexive, Mutual Trust and Partially Transitiveness.

In this section, we propose a Kuder – Richardson coefficient based trust mechanism. This mechanism has an ability of identifying and isolating malicious nodes which may disturb the service discovery process in an ad hoc environment. In this mechanism, the detection of malicious nodes is mainly based on a factor called Kuder-Richardson coefficient, which is similar to Cornbach alpha coefficient.

Let us consider the number of packets forwarded by 'n' nodes in 'k' sessions is given in eq., (1)

$$Y = y_1 + y_2 + \cdots + y_n. \qquad (1)$$

Then, the trust factor namely Kuder-Richardson coefficient (KRC) is manipulated by each node using the formula given in the (2)

$$r = \frac{k}{k-1}\left[1 - \frac{\sum_{i=1}^{k} P_i Q_i}{var(x)}\right] \qquad (2)$$

Here,

'r' - Kuder-Richardson coefficient

'k' -Number of sessions in service discovery

'p' -the chance of successful event of forwarding of neighbor packets

'q' -the chance of unsuccessful event forwarding of neighbor packets

'σ_x^2' – the variance computed based on the deviation between the total numbers of packets received by a node to the total number of packets relayed by that node.

Where,

$$\sigma_{x^2} = \frac{\sum_1^n (x_i - \bar{x})^2}{n}$$

Here, 'n' – The number of nodes present in the ad hoc network topology.

4. KUDER RICHARDSON COEFFICIENT BASED TRUST MODEL FOR ENHANCING SERVICE DISCOVERY IN MANETS

Notations:

SRN: Source Nodes

GDST: Group of Destination nodes

KRC: Kuder-Richardson based reliability Coefficient

1. The SRN broadcasts the packets through all possible paths available in the topology.
2. The DSG confirms with the help of RREP through reverse routes.
3. SRN then forwards Data to DGST through minimal path based on group id.
4. The adjacent neighbor nodes of each and every node are mentioned for manipulating the variance in packets for entire k sessions as well as for each session.
5. Then monitoring neighbor nodes by computing KRC with the help of equations (1), (2) and (3).
6. If ($0 \leq KRC \leq 0.3$) then.
7. Check the priority of service discovery
8. The node is malicious node
9. Call Rehabilitate the network();
10. Else
11. If ($0.31 \leq KRC \leq 1.0$) the node exhibits normal behavior.
12. Allow nodes for service discovery process.
13. Then, the neighbor confirms the node trust value.
14. Else
15. End if

Each and every node is monitored by their neighbor nodes based on the manipulation of a factor called KRC (Kuder-Richardson Coefficient) which is based on the deviation between the numbers of packets received and relayed by a node in the entire 'k' sessions. If this parameter is less than or equal to 0.3 then the node can be conformed as distrust or malicious node. Still, if KRC value is between 0.20 and 0.30 the nodes are even isolated during sensitive service discovery but for less significant service discovery the threshold range is between 0.10 to 0.19.

TABLE-I
Trust thresholds for nodes in service discovery for MANETS

S.No	Trust Threshold Range of nodes for enabling Services	Type of Communication supported
1	0.31 TO 1.0	Secure communication
2	0.21 TO 3.0	Non Secure communication (Least significant services)
3	< 0.21	Non Secure communication(Most significant services)

5. SIMULATION RESULTS AND DISCUSSIONS

The simulations of our trust based mechanism were carried out extensively with the network simulator tool ns-2.26.Our simulated ad hoc scenario consists of 50 mobile nodes deployed in a terrain size of 1000X1000 square meters. The results are manipulated depending on the aggregate of 20 simulation rounds. The number of packets used as maximum threshold for carrying out our study is 1000, which is quite sufficient for continuing the session up to the end of the simulation time. The refresh interval used for the simulation is 1 sec. Here the packet size transmitted from the source is 512 bytes and the wireless channel capacity is 2 Mbps.

A. *Metrics Used*

The extensive analysis of the devised Kuder-Richardson co-efficient aided trust based security mechanism for establishing service discovery in MANET were carried out based on the following evaluation metrics.

1) *Packet delivery ratio*: It is the ratio of the maximum number of packets received by the destination nodes to the actual number of packets generated from the source nodes for the destination nodes.

2) Control overhead: It is the maximum bytes of packets that are used for establishing effective communication between the source nodes and the group of destination nodes.

3) *Total overhead*: It is defined as the ratio of the aggregate sum of control packet and the data packet to the total sum of data packets that is forwarded towards the destination.

4) *Throughput*: It is defined as the total number of all the packets that reaches the destination node from the source node through the intermediate hops within a interval of time.

6. DISCUSSIONS.

B. Performance Evaluation for Kuder-Richardson co-efficient based trust mechanism (KRCBM) for service discovery in MANET:

i) Based on the number of malicious nodes set (10)

1) *Packet delivery ratio:* The performance of the protocol decreases when the number of malicious nodes existing in the scenario increases. Since, the performance of the protocol is inversely proportional to the existence of the selfish nodes; the need for the deployment of KRCBM arises. From the figure 1 it is obvious that the deployment of KRCBM in the AODV protocol shows a steady increase in performance in terms of Packet Delivery Ratio

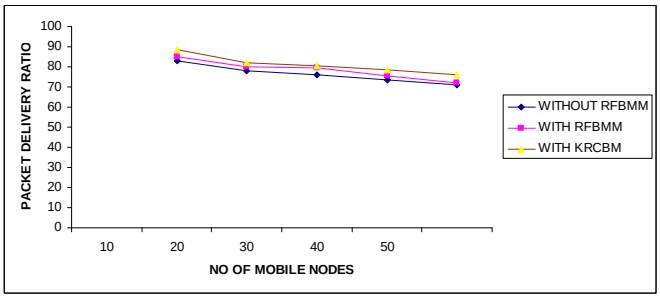

Figure 1 Performance analysis for KRCBM based on number of malicious nodes with respect to Packet delivery ratio.

This trust mechanism model shows a phenomenal increase of 21 % in Packet Delivery Ratio.

2) Control Overhead: The AODV protocol performance in terms of control overhead increases when the number of selfish nodes existing in the scenario increases. Since, the performance of the protocol with respect to the control overhead is directly proportional to the existence of the selfish nodes; the need for the deployment of KRCBM arises. From the figure 2 it is obvious that the deployment of KRCBM in the AODV protocol shows a steady decrease in the control overhead.

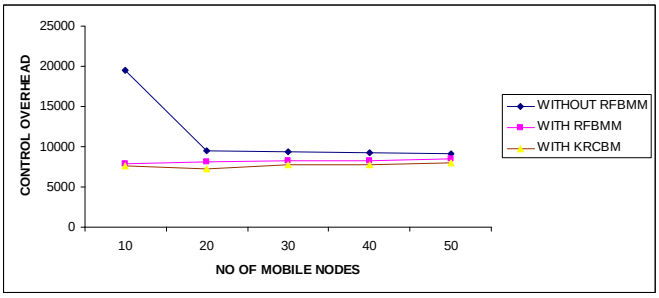

Figure 2 Performance analysis for KRCBM based on number of malicious nodes with respect to Control Overhead

This mathematical model shows a phenomenal decrease of 17 % in the Control overhead

3) *Total Overhead:* The AODV protocol performance in terms of total overhead increases when the number of selfish nodes existing in the scenario increases. Since, the performance of the protocol with respect to the total overhead is directly proportional to the existence of the selfish nodes, the need for the deployment of KRCBM arises. From the figure 3 it is obvious that, deployment of KRCBM in the AODV protocol shows a steady decrease in the total overhead.

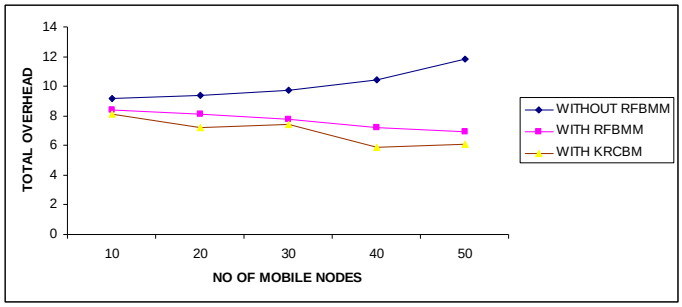

Figure 3 Performance analysis for KRCBM based on number of malicious nodes with respect to Total overhead

This mathematical model shows a phenomenal decrease of 23 % in the total overhead.

4) *Throughput:* The throughput of the AODV protocol decreases when the number of selfish nodes existing in the scenario increases. Since, the throughput of the protocol is inversely proportional to the existence of the selfish nodes; the need for the deployment of KRCBM arises. From the figure 4 it is obvious that the deployment of KRCBM in the AODV protocol shows a steady increase in the throughput.

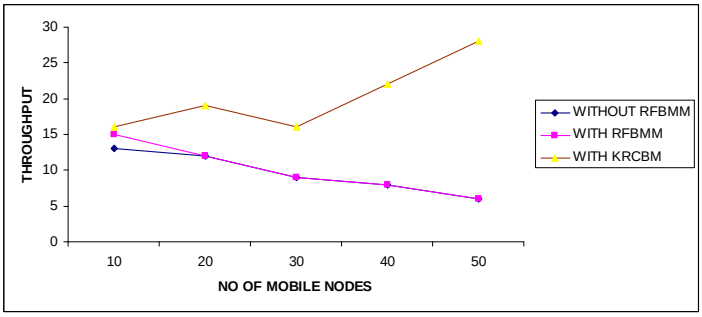

Figure 4 Performance analysis for KRCBM based on number of malicious nodes with respect to Throughput.

This trust mechanism shows a phenomenal increase of 23 % in Throughput.

ii) Based on the number of malicious nodes set (20)

1) *Packet delivery ratio:* The performance of the protocol decreases when the number of malicious nodes existing in the scenario increases. Since, the performance of the protocol is inversely proportional to the existence of the selfish nodes; the need for the deployment of KRCBM arises. From the figure 5 it is obvious that the deployment of KRCBM in the AODV protocol shows a steady increase in performance in terms of Packet Delivery Ratio.

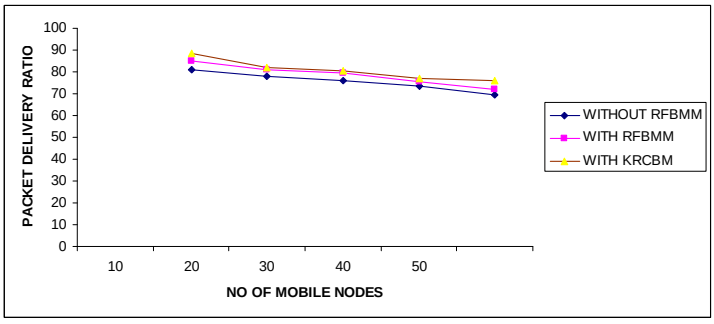

Figure 5 Performance analysis for KRCBM based on number of malicious nodes with respect to Packet delivery ratio.

This trust mechanism shows a phenomenal increase of 25 % in Packet Delivery Ratio.

2) Control Overhead: The AODV protocol performance in terms of control overhead increases when the number of selfish nodes existing in the scenario increases. Since, the performance of the protocol with respect to the control overhead is directly proportional to the existence of the selfish nodes; the need for the deployment of KRCBM arises. From the figure 6 it is obvious that the deployment of KRCBM in the AODV protocol shows a steady decrease in the control overhead.

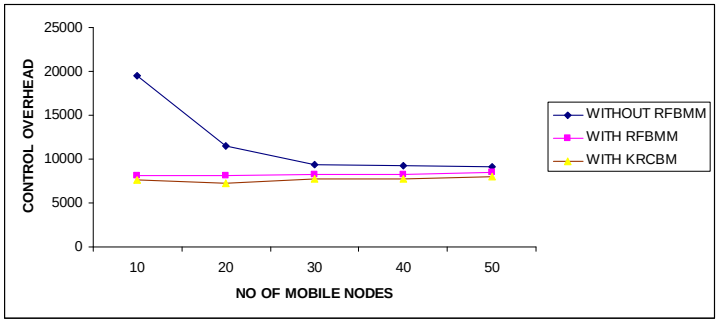

Figure 6 Performance analysis for KRCBM based on number of malicious nodes with respect to Control Overhead

This mathematical model shows a phenomenal decrease of 27 % in the Control overhead

3) *Total Overhead:* The AODV protocol performance in terms of total overhead increases when the number of selfish nodes existing in the scenario increases. Since, the performance of the protocol with respect to the total overhead is directly proportional to the existence of the selfish nodes, the need for the deployment of KRCBM arises. From the figure 7 it is obvious that, deployment of KRCBM in the AODV protocol shows a steady decrease in the total overhead.

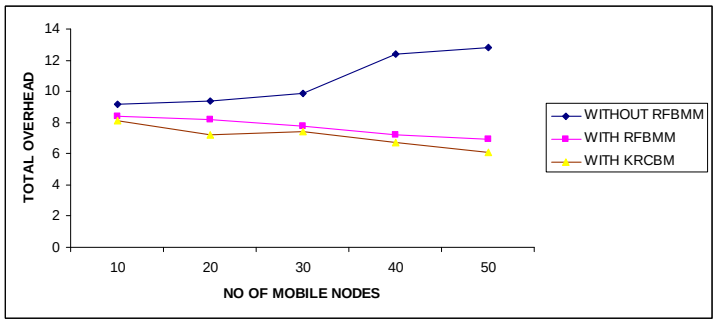

Figure 7 Performance analysis for KRCBM based on number of malicious nodes with respect to Total overhead

This mathematical model shows a phenomenal decrease of 18 % in the total overhead.

4) *Throughput:* The throughput of the AODV protocol decreases when the number of selfish nodes existing in the scenario increases. Since, the throughput of the protocol is inversely proportional to the existence of the selfish nodes; the need for the deployment of KRCBM arises. From the figure 8, it is obvious that the deployment of KRCBM in the AODV protocol shows a steady increase in the throughput.

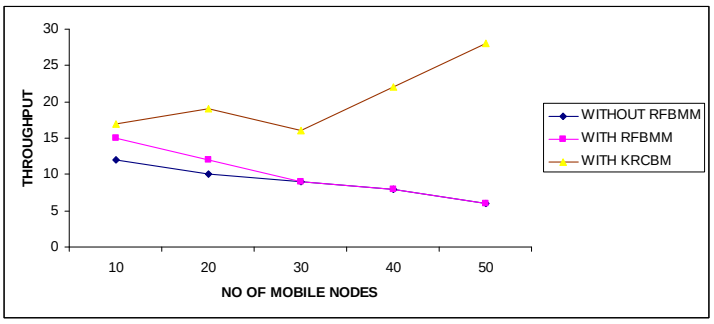

Figure 8 Performance analysis for KRCBM based on number of malicious nodes with respect to Throughput.

This mathematical model shows a phenomenal increase of 19 % in Throughput.

7. CONCLUSION

In this paper, we have presented a Kuder-Richardson co-efficient based trust mechanism (KRCBM) for service discovery in MANET, which is deployed omnipresent in each and every node of the network. The results of this proposed trust based mechanism for service discovery makes it obvious that it provides better performance in terms of Packet Delivery Ratio, Total overhead, Control overhead and Throughput. In the near future, new reputation mechanism for detecting the malicious nodes based on Alpha coefficient, Cohen's kappa Coefficient.

8. REFERENCES

[1] Sonja Buchegger Jean – Y ves Le Boudec, "A Robust Repudiation system for mobile ad-hoc networks," EPFL IC Technical Report IC/2003/05.

[2] P.Michiardi and R.Molva, "CORE: A collborative repudiation mechanism to enforce node coperating in mobile ad hoc networks," Proceeding of the 6th Joint working conference on communications and multimedia security, ,pp 107-121, September 2002.

[3] Alessandro Mei , Julinda Stefa, "Give 2Get: Forwarding in Social Mobile wireless networks of selfish Individual," IEEE Trasactions on dependable and secure computing, vol.9 No.4 pp 569 – 581, July/August 2012.

[4] S.Eidenbenz ,G.Resta, and P.Santi, "The Commit Protocol for truthful and cost – efficient Routing in Ad hoc networks with selfish nodes," IEEE Transaction on Mobile Computing, Vol 7, No. 1 pp. 19 - 32 January 2010.

[5] M.Tamer Refari, Vivek Srivatsava , Luiz DaSilva, Mohamed Eltoweissy,"A Repudiation - based Mechanism for isolating selfish nodes in Ad hoc Networks," Proceeding of Mobiquaitous '05, IEEE 2005.

[6] Ze Li, Haiying Shen, "Game – Theoretic analysis of cooperation EquiIncentive strategies in Mobile Ad hoc networks," IEEE Transl.on Mobile computing vol. 11, No 8 pp. 1287–1303, August 2012.

[7] Feng Li , Jie Wu , "Attack and Flee: Game –Theory – Based Analysis on Interactions Among Nodes in MANETs,"IEEE Transaction on System, Man and Cybernetics Vol 40, No 3 pp 612 – 622 June 2010.

[8] Shukor Abd Razak ,Normalia Samia, Mohd Aizia Maarof , "A Friend Mechanism for mobile ad hoc networks," The fouth International conference Information Assurance and Security, IEEE 2008.

[9] Hazer Inaltekin, Stephen B. Wicker ,"The analysis of Nash Equilibria of one shot Random – Access Game for wireless Networks and the behavior of selfish Nodes," IEEE Transactions on Networking ,Vol 16, NO.5 pp.1094-1170 ,October 2008.

[10] Joseph A.Gliem, Rosemary R. Gliem, "Calculating, Integrating , and Reporting Cronbach's Alpha Reliability coeeficient for Likert –Type Scales," In proceedings of MRPC, Vol 4, pp 82- 882003

[11] Paul Dressal,"Some remarks on kuder-richardson reliability coefficient," phychometrica, Springer, Vol 8(4),pp 223-245,December 1999.

[12] Lawrence M.Healey, "Logistic Regrssion : An Overview," In Proceeding of COT 07 11,Vol.2, pp 30-37, March 2006.

[13] Chong Ho Yu, "An introduction to computing and interpreting Cronbach coefficient alpha in SAS," IEEE 2005