ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

Probe Packets Based Fault Tolerant Scheme for Service Discovery in Manets

[I]Dr.G.Seenuvasan, [II]D.Bharathi
[I]Asst. Professor, Dept. of Computer Sc., Swami Vivekanantha Arts & Science College, Villupuram, Tamilnadu, India
[II]M.Phil. Research Scholar, Thiruvalluvar University, Tamilnadu, India

Abstract
In MANETs, each and every route established between the source and the destination is relied to carry large amount of traffic and hence failures may drastically interrupt the end-user due to the lack of central authority. Hence, providing fault-tolerance mechanism for enhancing the service discovery becomes an issue for this multi-hop wireless networks. In this paper, we propose a reliable and fault-tolerant routing algorithm called Probe Packets Based Fault Tolerant Scheme for Service Discovery Mechanism (PPBFTS) for establishing primary and backup paths during failure caused by untrustworthy nodes. This PPBFTS mechanism uses both primary path and backup path for fault tolerance in which the primary path is established using load balancing approach while the backup path setup calculates the blocking probability of the existing paths. Based on the simulation results, it is obvious that our PPBFTS reduces the blocking probability and latency while increasing the throughput. We also analyze the performance of this mechanism, PPBFTS using ns-2.26 network simulator with CONFIDANT protocol based on evaluation metrics such as packet delivery ratio, throughput, total overhead and control overhead.

Keywords
Packets Based Fault Tolerant Scheme for Service Discovery Mechanism, Secure Service Discovery Based on Probe Packet Mechanism, Probe's Trust Factor.

I. Introduction

In MANETs, each and every route established between the source and the destination is relied to carry large amount of traffic and hence failures may drastically interrupt the end-user due to the lack of central authority. Hence, providing fault-tolerance mechanism for enhancing the service discovery becomes an issue for this multi-hop wireless networks. In this paper, we propose a reliable and fault-tolerant routing algorithm called Probe Packets Based Fault Tolerant Scheme for Service Discovery Mechanism (PPBFTS) for establishing primary and backup paths during failure caused by untrustworthy nodes. This PPBFTS mechanism uses both primary path and backup path for fault tolerance in which the primary path is established using load balancing approach while the backup path setup calculates the blocking probability of the existing paths. Based on the simulation results, it is obvious that our PPBFTS reduces the blocking probability and latency while increasing the throughput. We also analyze the performance of this mechanism, PPBFTS using ns-2.26 network simulator with CONFIDANT protocol based on evaluation metrics such as packet delivery ratio, throughput, total overhead and control overhead.

II. 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 enability 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

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

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.

III. Proposed Solution

A. Overview

In the proposed mechanism, source node initiates the route discovery process towards the destination nodes when it has some data to be sent. The source node first sends RREQ's to all its neighbors with its own source id and the destination id for which the packets are actually destined for. Once the optimal route is established between the source node and the required destination nodes, probing of packets come into play. This solution guarantees that multicast data is delivered from source to the members of the multicast group, even in the presence of attackers and it also ensures that only authorized nodes perform certain operations (like tree nodes performing tree operations and group nodes connecting to the corresponding multicast tree). This solution is also capable of mitigating attacks that try to prevent a node from establishing a route to the multicast tree both in route request and route reply. A new parameter PTF (Probe's Trust Factor) is used to choose the best path which ensures trustworthiness of the path by calculating the trust value of the neighbor nodes which is later stored in a trust table. When a node wants to join a multicast group, it sends the route request to the desired group and then the entries are updated in the multicast table on calculating the trust value of the node. The trust table gathers the information about the data and control packets of its neighboring node and overhears data whether a packet of control message is dumped and not retransmitted. Based on this, every node is set to maintain some values in a table for its neighboring node. The trust level can be calculated based on the events are recorded. Based on the factors represent the reliability of the particular event which varies in the ranges from higher priority to lower priority. Negative values for trust can take place as a result of more failures than success for an event. Hence, a trust value of '-1' represents complete distrust, '0' implies noncontributing event and '1' means absolute trust in a particular event. The trust values are then assigned weights to determine the aggregate trust level for another node. The trust values can be calculated as

TV=W(RREQ)*Qr+(MACT)*Qm+W(GRPH)*Qg

Where function W is the weight value of corresponding packet category. These values are dynamically updated based on the successful delivery of a packet on receiving an error message. Upon receiving the route replies, best path will be chosen by the source depending on the average trust level TV (avg) value of the entire path which can be calculated as

TV (avg) = TV / Hop count

Every source will maintain a table named average trust value table which contains destination host, next hop and average trust level for the existing paths. These values are updated based on the sent RREQ messages. This solution prevents malicious nodes from being a part of a multicast tree or from joining a multicast tree. Each node forwards RREQ only when the node from which RREQ received must be a trusted node.

A node will respond to RREQ if both the trust value and processing priority are high. If they are low, the victim node will deny the RREQ packet from the attacker.

In this solution, each node calculates the processing priority for all its neighbor nodes. Processing priority is inversely proportional to its rate of origination of RREQ packets. Threshold is the maximum of generation of RREQ in a period of time. Obviously the attacker's priority will be very low because the attacker continuously floods the RREQ without any time constraint. Along with that processing priority, each node should calculate the trust value. The solution assumes that the nodes are already authenticated and hence participate in communication. Assuming this condition, the flooding attack is discussed, the approach to prevent the flooding attack is to make use of a '*Trust Table*' wherein every participating node will be assigned a trust level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a '*attacker node*' and it is eliminated.

The source node transmits the RREQ to all its neighbors. Then the source waits for 'TIMER' seconds to collect. A RREQ is chosen based on the following criteria, in each of the received RREQ, the trust level of the responding node, and each of its next hop's level are checked. If two or more routes seem to have the same trust level, then select the one with the least hop count; else, select the one with the highest level. The trust levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to the source, whereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented. A valid route is selected from the received responses based on the following methodology. A trust table is maintained that will hold the trust levels of the participating nodes. The basic idea is to select the node with a high trust level.

Initially, the trust levels of the responded node and its next hop are looked for. If the average of their levels is found to be the highest of all trust levels, then the node is considered to be reliable. On the receipt of multiple responses, the one with the highest trust level is chosen. In case, two or more nodes seemed to have the same trust levels, then the one with the minimum hop count is chosen. The source S chooses the response RREQ which has the highest trust value and shortest number of hops to the destination.

IV. Probe Packets Based Fault Tolerant Scheme For Service Discovery In Manets.

PPBFTS algorithm:

RREQ : Route Request
RREQ_COLLECT_TIME: Time for which responses(route replies) are collected
IN : Intermediate Node
ACK_TIMEOUT: Time for which a node waits for ACK source broadcasts RREQ

```
While(simclock=current_time+RREQ_COLLECT_TIME)
  {
Store in RREQT
}
if (size of RREQT = 0)
{
retransmit RREQ
}
else
{
find AVG_TRUST_LEVEL = TRUST LEVEL IN + TRUST LEVEL next hop
select route with highest AVG_TRUST_LEVEL
if(two or more RREQ has same highest AVG_TRUST LEVEL)
select the one which has lowest hop count
if(two or more RREQ has same hop  count)
select the one from highest level
send RREQ to next hop
}
while(simclock=current_time+ACK_TIMEOUT)
{
if RACK is received
{
  increment the trust level of the IN and next hop
  broadcast the trust table find the optimal average distance.
}
}
if (no RACK is received)
{
decrement the trust level of the IN and next hop
broadcast the trust table
}
if (TRUST LEVEL of a node = 0)
{
    remove the node fro m RREQ table and trust table
    broadcast alarm packets
}
```

V. Simulation Study

The performance of SSDPPM is studied based on the network simulation using ns-2.26. In our simulation, we are simulating a scenario of 50 nodes in square area of 1,000m x 1,000m. The mobility model is random waypoint model. At the beginning, each node has random initial location, it will move to random destination with random speed. Simulation runs for 50 seconds. Each session is for 10 Seconds

A. Performance Metrics

In case of group communication, the reliability of data transfer depends on the root node of each multicast group. Hence, the presence of DoS attack disturbs the packet delivery, whereas increases the number of retransmissions. Hence this detection and mitigation algorithm as to be evaluated based on the parameters discussed below.

Packet Delivery Ratio: Packet delivery ratio is defined as the ratio of data packets received by the mobile node in the destinations to those generated by the sources.

Throughput: It is defined as the total number of packets delivered over the total simulation time.

Total Overhead: It is the ratio of total number of packets necessary for connection establishment and data delivery to the number of data packets that reaches the destination.

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

The following table 1 illustrates the simulation parameters that are set for our stud

Table 1: Simulation Parameters

Parameter	Value	Description
No. of mobile nodes	50	Simulation Node
Type of Protocol	AODV	Ad hoc On-demand Distance Vector Protocol
Type of Traffic	40 packets per Second	Constant bit rate
Type of Propagation	Two Ray Ground	Radio propagation model
Simulation Time	50m	Maximum simulation time.
Number of packets used	1000	Maximum number of packets used in simulation.
Channel capacity	2 Mbps	Capacity of the wireless channel

B. Performance analysis for PPBFTS based on varying number of Mobile Nodes:

The performance analysis of PPBFTS over CONFIDANT and SSDPPM is studied based on two experiments, In which the first experiment is based on 10 attacker nodes while the second experiment is carried out with 20 attacker nodes.

Experiment 1: Performance analysis for PPBFTS with 10 attacker nodes

1. Packet Delivery Ratio: The figure 1 provides the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on packet delivery ratio. Our proposed mechanism, PPBFTS shows increase in the packet delivery ratio than CONFIDANT from 5% to 14% and from 21% to 34% over SSDPPM.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

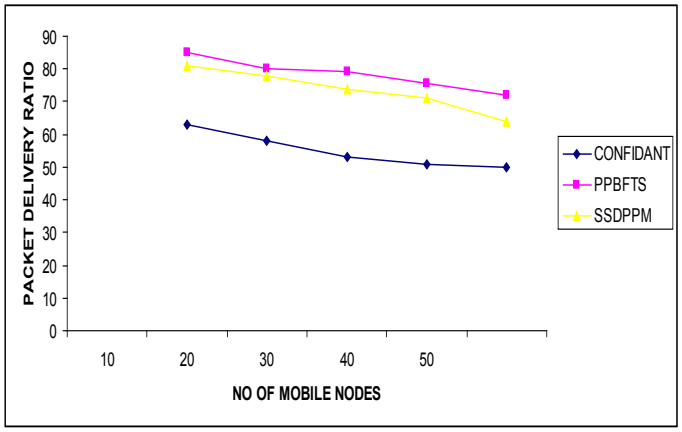

Fig.1: Comparison Chart for PPBFTS based on Packet Delivery Ratio

Hence, it is obvious that PPBFTS is considered as an effective approach which mitigates the malicious nodes and provides fault tolerance for enhanicng the service discovery by increasing the packet delivery rate in an average of 23%.

2. Throughput: The following figure 2 illustrates the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on throughput . Our proposed mechanism, PPBFTS shows increase in throughput than CONFIDANT from 15% to 23 % and from 24% to 31% over SSDPPM.

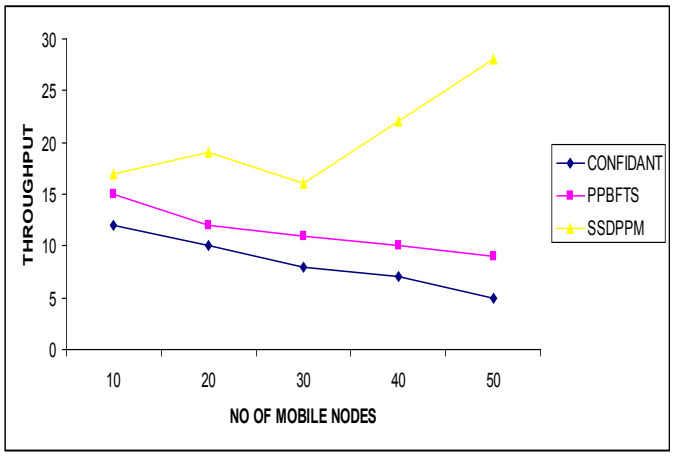

Fig. 2: Comparison Chart for PPBFTS based on Throughput

Hence, it is obvious that our PPBFTS can be considered as an effective approach which mitigates the malicious nodes and thus increases the throughput in an average of 21%.

3. Total Overhead: The following figure 3 illustrates the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on total overhead .Our proposed mechanism, PPBFTS shows a decrease in total overhead than CONFIDANT from 24 % to 28 % and from 28% to 36 % over SSDPPM.

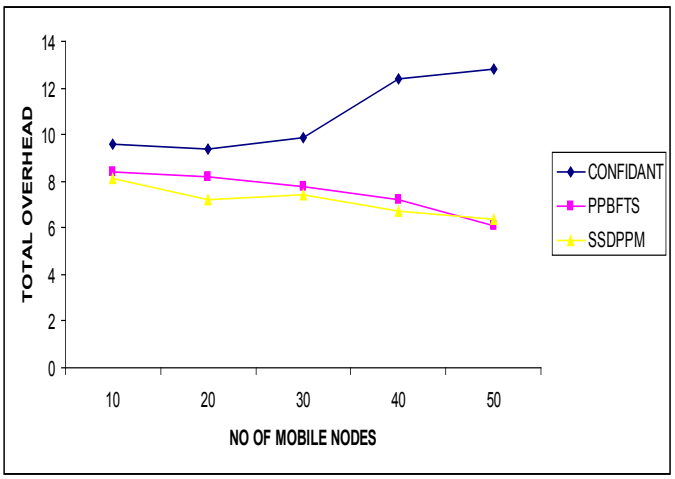

Fig. 3: Comparison Chart for PPBFTS based on Total Overhead

Hence, it is obvious that PPBFTS can be considered as effective approach which mitigates the malicious nodes present in an ad hoc environment and thereby reduces the total overhead in an average of 26 %.

4. Control Overhead: The following figure 4 illustrates the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on control overhead .Our proposed mechanism, PPBFTS shows a decrease in control overhead than CONFIDANT from 20 % to 25 % and from 27% to 33 % over SSDPPM.

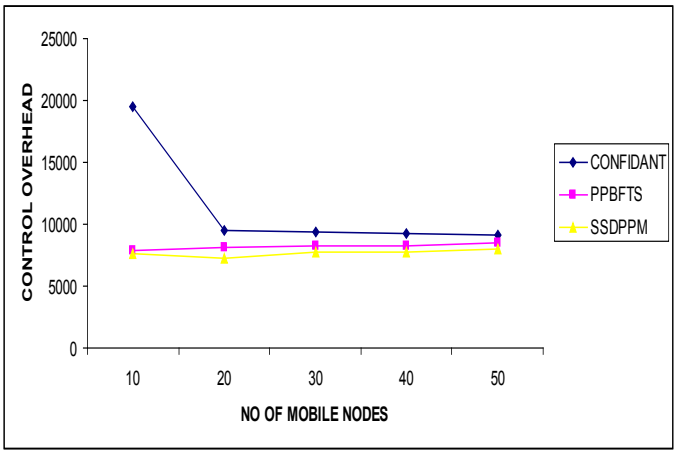

Fig. 4: Comparison Chart for PPBFTS based on Control Overhead

Hence, it is obvious that PPBFTS can be considered as an effective approach which mitigates the malicious malicious nodes present in an ad hoc environment and thereby reduces the number of retransmissions in an average of 24%.

Experiment 2: Performance analysis for PPBFTS with 20 attacker nodes

1. Packet Delivery Ratio: The following figure 5 illustrates the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on packet delivery ratio. Our proposed mechanism, PPBFTS shows increase in the packet delivery ratio than CONFIDANT from 16% to 21% and from 25% to 29% over SSDPPM.

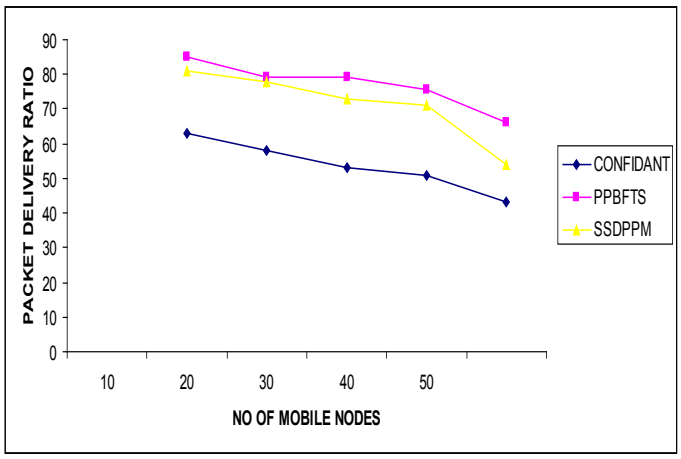

Fig. 5: Comparison Chart for PPBFTS based on Packet Delivery Ratio

Hence, the PPBFTS could be considered as an effective mechanism in the mitigation of root node attack, since in an average this mechanism shows phenomenal increase of 21 % in packet delivery ratio.

2. Throughput: The following figure 6 illustrates the comparative analysis of of PPBFTS with CONFIDANT and SSDPPM based on throughput . Our proposed mechanism, PPBFTS shows increase in throughput than CONFIDANT from 18% to 27 % and from 29% to 36% over SSDPPM.

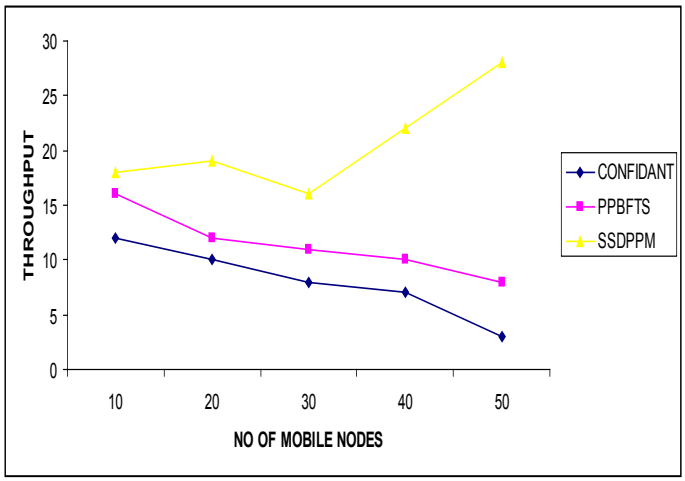

Fig. 6: Comparison Chart for PPBFTS based on Throughput

Hence, the PPBFTS could be considered as an effective mechanism in the mitigation of root node attack, since in an average this mechanism shows phenomenal increase of 25% in throughput.

3. Total Overhead: The following figure 7 illustrates the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on total overhead .Our proposed mechanism, PPBFTS shows a decrease in total overhead than CONFIDANT from 18 % to 24 % and from 25% to 34 % over SSDPPM.

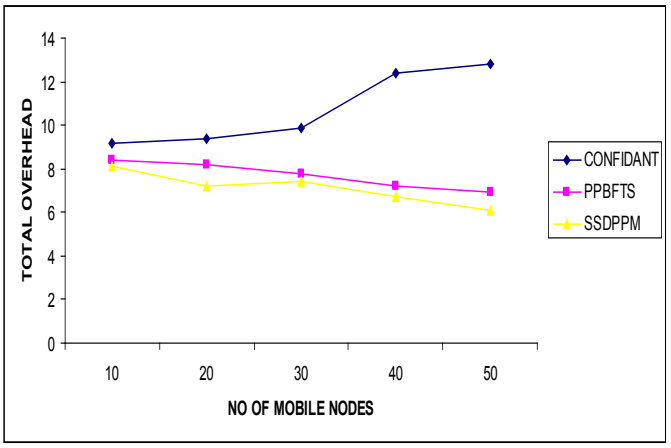

Fig.7 : Comparison Chart for PPBFTS based on Total Overhead

Hence, it is obvious that PPBFTS can be considered as effective approach which mitigates the malicious nodes present in an ad hoc environment and thereby reduces the total overhead in an average of 22 %.

4. Control Overhead: The following figure 8 illustrates the comparative analysis of PPBFTS with CONFIDANT and SSDPPM based on control overhead .Our proposed mechanism, PPBFTS shows a decrease in control overhead than CONFIDANT from 24 % to 29 % and from 30% to 34 % over SSDPPM.

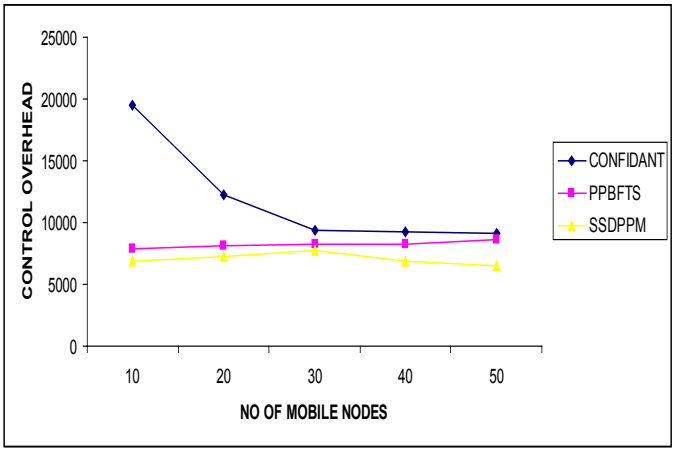

Fig. 8: Comparison Chart for PPBFTS based on Control Overhead

Hence, it is obvious that PPBFTS can be considered as an effective approach which mitigates the malicious malicious nodes present in an ad hoc environment and thereby reduces the number of retransmissions in an average of 31 %

IV. Conclusions

In this paper, we have presented a called Probe Packets Based Fault Tolerant Scheme for Service Discovery Mechanism (PPBFTS) for establishing primary and backup paths during failure caused by untrustworthy nodes. From the simulation study, it is obvious that our PPBFTS provides better performance in terms of packet delivery rate, Total overhead, Control overhead and Throughput when compared to CONFIDANT and SSDPPM mechanism present in the literature for providing fault tolerance in an ad hoc environment. In the near future, new probe packet based service discovery mechanism based on fault tolerant measure

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

for isolating the malicious nodes based on Kuder-Richardson-21 may be incorporated.

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.*

[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*

Author's Profile

Dr. G.Seenuvasan received his Doctorate Award by university of global peace for the excellence in social service. He has received his M.Phil,Degree from Prist university, in the year 2011. He has received his M.C.A Degree from Anna University, Chennai in the year 2010. He is working as Asst.Professor, Swami Vivekanandha Arts and Science College, Orathur,Villupuram, Tamilnadu.

Ms.D.Bharathi M.Phil(C.S) Degree from Thiruvalluvar University,Vellore. She has received her M.C.A Degree from Anna University,Chennai in the year 2010.

Address for Communication:
Dr.G.Seenuvasan,
No.2/18, Thenkolapakkam Village,
Mailam Post, Tindivanam T.K., 604304,
Villupuram District, Tamilnadu, India.
PH: 09677835172, 08608335172
EMAIL: seenu0301g@gmail.com