DOI: 10.21917/ijct.2015.0154

SECURE SERVICE DISCOVERY BASED ON PROBE PACKET MECHANISM FOR MANETS

S. Pariselvam[1], G. Madhubala[2] and R.M.S. Parvathi[3]
[1,2]*Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, India*
E-mail: [1]s.pariselvam@gmail.com, [2]madhubalaifet@gmail.com
[3]*Department of Computer Science and Engineering, Sengunthar College of Engineering, India*
E-mail: parvathi.info@scew.org

Abstract

In MANETs, Service discovery process is always considered to be crucial since they do not possess a centralized infrastructure for communication. Moreover, different services available through the network necessitate varying categories. Hence, a need arises for devising a secure probe based service discovery mechanism to reduce the complexity in providing the services to the network users. In this paper, we propose a Secure Service Discovery Based on Probe Packet Mechanism (SSDPPM) for identifying the DoS attack in MANETs, which depicts a new approach for estimating the level of trust present in each and every routing path of a mobile ad hoc network by using probe packets. Probing based service discovery mechanisms mainly identifies a mobile node's genuineness using a test packet called probe that travels the entire network for the sake of computing the degree of trust maintained between the mobile nodes and it's attributed impact towards the network performance. The performance of SSDPPM is investigated through a wide range of network related parameters like packet delivery, throughput, Control overhead and total overhead using the version ns-2.26 network simulator. This mechanism SSDPPM, improves the performance of the network in an average by 23% and 19% in terms of packet delivery ratio and throughput than the existing service discovery mechanisms available in the literature.

Keywords:

MANET, SSDPPM, DoS

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.

Form 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]. In this proposed schema, we employ a Secure Service Discovery Based on Probe Packet Mechanism (SSDPPM) for identifying the DoS attack in MANETs. Here, the protocol used for carrying out is analysis is the tree based and reactive protocol called AODV. This protocol is the most widely used protocol due to its high flexibility for incorporating secure and robust mechanisms.

The remaining part of the paper is organized as follows. In section 2, we enumerate the related works present in the literature with a brief consolidation of the survey. The detailed description of the proposed Secure Service Discovery Based on Probe Packet Mechanism (SSDPPM) is depicted in section 3. The algorithm of the proposed Probe Packet Mechanism (SSDPPM) for service discovery is presented in section 4. The Simulations setup and the simulation results are presented and studied in section 5 and 6. Section 7 concludes the paper.

2. RELATED WORK

In the literature, researchers have proposed various trust based mechanisms which facilitates reliable data transmission in ad hoc networks. These mechanisms were broadly classified into two categories viz., first hand trust based reputation mechanism and second hand trust based mechanism. Some of the above said approaches were discussed below.

A multilevel trust based mechanism which incorporates faithful behavior of a mobile node for service discovery has been proposed by Alessandro Mei and Juliana Stefan in paper [3]. This processing of this mechanism reduces the number of duplicates results in reduced spatial complexity which in turn enhances the performance of the network. The main drawback of this mechanism is that, it works in an assumption that the all the mobile nodes will not deviate from their normal behavior. Further, Stephan Eidenbenz et al, [4] proposed a distributed algorithm for optimal service discovery. Authors have formulated this mechanism mainly based on the four different postulates of the mobile node such as the behavior of the mobile node in routing, the genuineness of the mobile nodes participating in the routing, Transmission of packet through energy efficient and shortest paths, Transmission of a message with less overhead. Authors also implemented a VCG payment scheme based on game theoretic technique to achieve the reliable transmission in the entire network.

Furthermore, Tamer Rafael et al. [5] proposed a reputation mechanism, which works when deployed in all the nodes present in an ad hoc network. Authors have introduces two new concepts viz., reputation index and reputation table which are incorporated by all the mobile nodes in the network. The reputation index of a mobile node is monotonically increasing value as when each and every packet is delivered successfully, whereas reputation table stores the values of reputation index with respect to sessions of transmissions. Authors have also contributed heuristics based approaches such as Hops away from source, double decrement/single increment ratio and random early probation.

Additionally, Ze Li and Haiying Shen, [6] proposed a trust oriented service discovery mechanism which incorporates a

factor known as reputation threshold factor in order to differentiate the reliable and non-cooperative nodes. Authors have also implemented a virtual cash mechanism for managing packet servicing activity for each and every mobile node. This mechanism is formulated based on game theory and hence it acts as a unified approach for service discovery in the presence of malicious nodes. Feng Li et al, [7] proposed a game theory trust mechanism which improves the interaction between the mobile nodes present in the routing path of the network. Authors also incorporated a Bayesian signaling game for identifying the contrast between the cooperative nodes and non-cooperative nodes in the dynamic scenario. This mechanism also incorporates the concepts like sequential rationality and randomness property for effective service discovery.

Yet, Shakur et al, [8] presented a mechanism which enables the degree of cooperation among the mobile nodes based on the estimation of the availability of their stringent resources. Authors incorporated a new concept known as friendship mechanism which is more useful in reducing the number of false positives in service discovery which occurs due to the presence of non-cooperative nodes. This mechanism has mainly handles six level of separations faced by each and every mobile node while participating in the routing process. The reputation factor of every mobile node is estimated through direct and indirect reputation mechanisms. Authors also implemented a voting strategy to distinguish between the genuine and non-cooperative node.

Yet another, Hazer Inaltekin and Stephen B. Wicker [9] enumerated various problems that arise in the scenario of service discovery and these problems are mainly due to the lack of co-ordination between the nodes in an ad hoc scenario. Authors formulated a game based theoretic solution based on Lévesque measure which assigns a probability value for each and every node participating in the route discovery activity. Authors have also quantified the performance of the network based on Nash Equilibrium function.

3. PROPOSED SOLUTION

3.1 OVERVIEW

In the proposed mechanism, the probing mechanism utilized for evaluating the trust of the nodes present at the intermediate routers of information between the source and the destination involves three phases such as history acknowledgement phase, history normalization phase and trust analysis phase.

In the history acknowledgement phase, Source node injects probe packets through all the possible paths towards the destination nodes. The probing mechanism in this phase is a reactive approach, (i.e. the information to be collected by the probes) depends on the type of misbehavior that each intermediate nodes exhibit during service discovery. In the case of service discovery, the presence of DoS attack in a node denies for forwarding packets to the neighbor nodes but receives the packets from its neighbours. The initial probe packet information is equal to the number of information's collected for inferring the maliciousness. The history acknowledgement predicting a node's capacity factor of forwarding "COF" possessed by a each and every node present on the routing path obtained through the probe packets for session 'n' is collected by means of Eq.(1).

$$\text{COF} = \frac{\text{No. of Packets received by a node in a session}}{\text{No. of packets forwarded by that node in that session}} \quad (1)$$

In the second phase called history normalization phase, the COF calculated for each session out of, 'n' session are classified into Max COF (MAX_f), Min COF (MIN_f), and Contextual COF ($CCOF_f$).based on the types of COF obtained the normalized $NCOF_f$ could be useful to produce an estimate. This estimate called $NCOF_f$ is manipulated based on Eq.(2).

$$NCOF_f = \frac{CCOF_f - MIN_f}{MAX_f - MIN_f} \quad (2)$$

From the $NCOF_f$ calculated, the trust of the path is evaluated through the values 0 or 1. In the last called trust analysis phase, each and every path's $NCOF_f$ if compared with other paths $NCOF_f$ value and if the value of $NCOF_f$ is comparatively very high. i.e., above a threshold value of deviation in trust framed as 0.65 then, the particular route is malicious, hence packet forwarding through that path is avoided to enable reliable service discovery.

In general, Probe packets are classified into two types such as passive and active probe packet. In this mechanism both Active and Passive probing are used for accessing both the local and global information obtained by observing the behavior of the whole network.

4. SECURE SERVICE DISCOVERY BASED ON PROBE PACKET MECHANISM (SSDPPM) FOR IDENTIFYING THE DOS ATTACK IN MANETS

Notations:

SRC: Source Nodes

DSN: Group of Destination nodes

COF: Capacity Factor of Forwarding.

Step 1: The SRC sends RREQ's to all its neighbors with its own source id and the destination id for which the packets are actually destined.

Step 2: When the DSN confirms with the help of RREP through reverse routes.

Step 3: The probing mechanism gets enabled, which evaluates the trust of the nodes present as the intermediate routers of information between the source and the destination.

Step 4: Initially, the SRC injects probe packets through all the possible paths towards the destination nodes.

Step 5: This probing mechanism in this phase is a reactive approach, (i.e. the information to be collected by the probes) depends on the type of misbehavior that each intermediate nodes exhibit during service discovery.

Step 6: In the case of service discovery, the presence of DoS attack in a node denies for forwarding packets to the neighbor nodes but receives the packets from its neighbours.

Step 7: The initial probe packet information is equal to the number of information's collected for inferring the maliciousness.

Step 8: The history acknowledgement predicting a node's capacity factor of forwarding "COF" possessed by a each and every node present on the routing path obtained through the probe packets for session 'n'

Step 9: In the second phase, the COF calculated for each session out of, 'n' session are classified into Max COF (MAX_f), Min COF (MIN_f), and Contextual COF ($CCOF_f$).based on the types of COF obtained the normalized $NCOF_f$ could be useful to produce an estimate.

Step 10: $NCOF_f$ calculated is the trust of the path which evaluates to the value 0 or 1.

Step 11: Finally, in the trust analysis phase, each and every path's $NCOF_f$ if compared with other paths $NCOF_f$ value.

Step 12: If the value of $NCOF_f$ is comparatively very high. i.e, above a threshold value of deviation in trust framed as 0.65.

Step 13: Then, the particular route is malicious, hence packet forwarding through that path is avoided to enable reliable service discovery.

Step 14: Else

Step 15: The node is malicious node

Step 16: Call Rehabilitate the network ();

Step 17: End

Step 18: End if.

Here, the number of probe packets is considered to be P_n and R_{tn} is the average rate of transmission of probe packets so that input probe packet gap is T_{in} for gathering the information about node's genuineness for each session.

5. SIMULATION STUDY

The proposed SSDPPM approach is investigated through the network simulator of version ns-2.26. This simulation environment contains 50 mobile nodes randomly distributed in the terrain network size of 1000 × 1000. Further, the channel capacity, refresh interval time and simulation time for the study is considered as 2 Mbps, 10 seconds and 100 seconds respectively. Furthermore, each source is assumed to transmit packets with a constant bit rate of 40 packets/sec.

5.1 PERFORMANCE METRICS

The mobile node during group communication in an ad hoc network mainly relies on the rate of data dissemination achieved through the genuine rendezvous root node of the multicast group. Hence, the presence of DoS attack disturbs the packet delivery, whereas increases the number of retransmissions. Thus, this service discovery process is evaluated based on the network related parameters as given 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 defined as the ratio of sum of data packets and control packets utilized for communication to the maximum number of data packets received at the 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 study.

Table.1. Simulation Parameters

Simulation parameters	Value	Description
No. of mobile nodes	50	Nodes used for simulating SSDPPM
Protocol Used	AODV	Ad hoc On-demand Distance Vector Protocol
Traffic type utilized	40 packets per Second	Constant bit rate
Type of Propagation	Two Ray Ground	Two ray ground is used as the radio propagation model.
Time of Simulation	50m	simulation time for running the simulator
Maximum number of packets utilized	1000	Maximum number of packets used in simulation.
Wireless channel capacity	2 Mbps	Capacity of the wireless channel

5.2 PERFORMANCE ANALYSIS FOR SSDPPM BASED ON VARYING NUMBER OF MOBILE NODES

Two experiments were conducted to assess the performance of the proposed SSDPPM approach. Both the experiments were conducted by considering the simulation environment with 100 mobiles nodes. In the first experiment, among 100 mobile nodes 10 nodes were considered as attacker nodes while the second experiment is carried out using 20 attacker nodes.

Experiment 1:

The main goal of this experiment is to evaluate the performance of proposed SSDPPM based on three scenarios such as AODV with Confident, AODV with ATTACK and AODV without ATTACK.

The following Fig.1 shows the plots obtained for the packet delivery ratio obtained by above said scenario implantation. The proposed approach increases the PDR at the rate from 5% to 14% than from AODV with Confident and from 21 to 34% AODV with attack, while AODV without attacks is an ideal case. On the whole, this approach shows increase in PDR at the average rate of 11% when compared with the existing method.

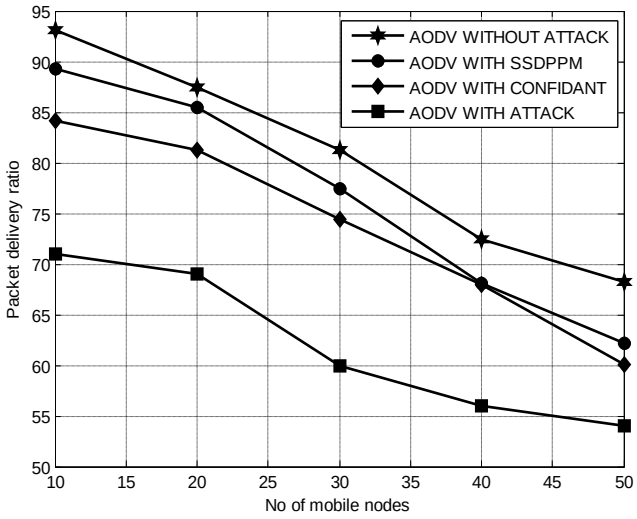

Fig.1. Performance Assessment Chart for SSDPPM based on Packet Delivery Ratio

The performance assessment of the proposed SSDPPM is analyzed by deriving throughput of the network in the above mentioned three difference scenarios. The Fig.2 illustrates the plots depicting throughput values obtained through AODV with SSDPPM, AODV with CONFIDANT, AODV with attack and AODV without attack. The proposed SSDPPM shows considerable increase in the throughput of the entire network from 6% to 12 % over AODV with CONFIDANT and 8% to 15% over AODV with ATTACK. From the results, it is clear that the proposed SSDPPM approach mitigates the attacker nodes present in that ad hoc environment in a rapid manner and increases the throughput to the average value of 7%.

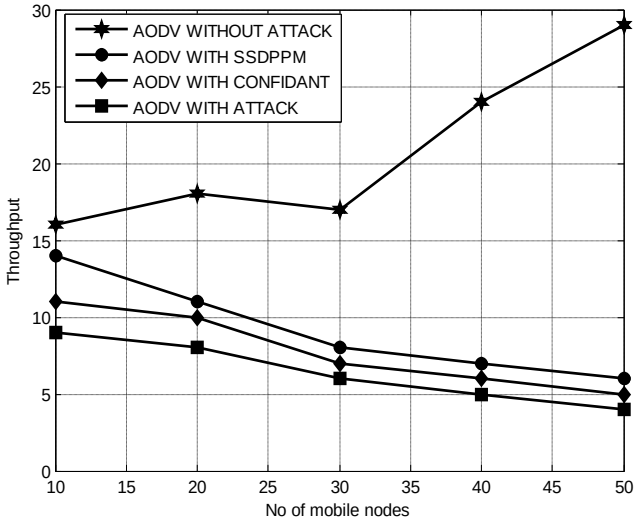

Fig.2. Performance Assessment Chart for SSDPPM based on Throughput

The performance of SSDPPM is further studied by deriving the values of total overhead of the network environment. The following Fig.3 shows the plots of total overhead values derived from all the three scenarios viz., AODV with SSDPPM, AODV with CONFIDANT, AODV WITH ATTACK and AODV WITHOUT ATTACK. The proposed approach AODV WITH SSDPPM significantly decreases the total overhead of the network at the rate from 3% to 6% over AODV with CONFIDANT and from 10% to 17% over AODV WITH ATTACK.

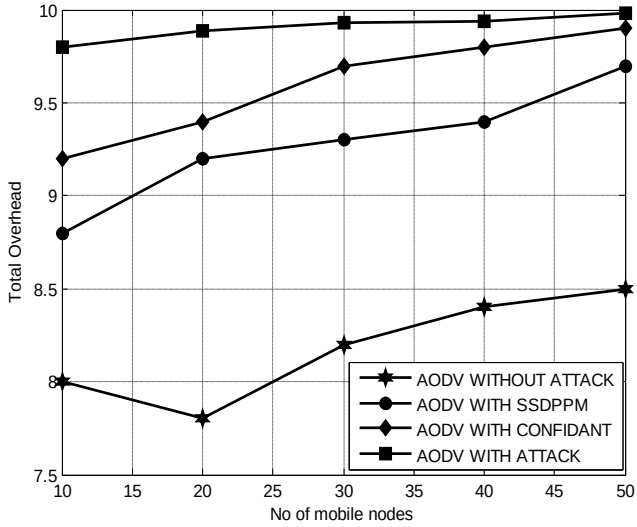

Fig.3. Performance Assessment Chart for SSDPPM based on Total Overhead

Moreover, the proposed SSDPPM approach reduces the total overhead at the average rate of 16% by mitigating the attackers nodes present in the routing path.

Finally, the performance assessment of the proposed SSDPPM is analyzed by means of measuring control overhead values of the ad hoc environment. The Fig.4 illustrates the plots depicting the control overhead values derived from all the three scenarios. The proposed SSDPPM approach decreases the control overhead of the network at the rate from 3% to 12% over AODV WITH CONFIDANT and from 6% and 17% over MAODV WITH ATTACK.

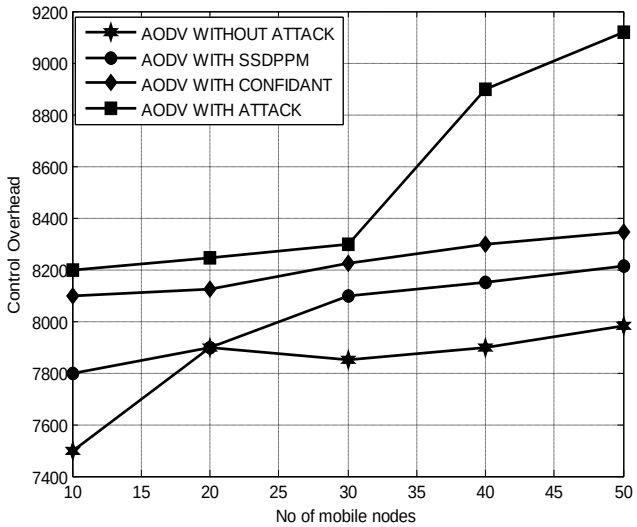

Fig.4. Performance Assessment Chart for SSDPPM based on Control Overhead

Hence, it is clear that the proposed SSDPPM approach mitigates the attacker nodes in the rapid manner and reduces the control overhead rate of the network to an average value of 14%.

5.3 PERFORMANCE ANALYSIS FOR CARCRM OBTAINED BY VARYING THE NUMBER OF MOBILE NODES

The following Fig.5 shows the plots obtained for the packet delivery ratio obtained by above said scenario implantation. The proposed approach increases the PDR at the rate from 5% to 14% than from AODV with Confident and from 21 to 34% AODV with attack, while AODV without attacks is an ideal case. On the whole, this approach shows increase in PDR at the average rate of 11% when compared with the existing method.

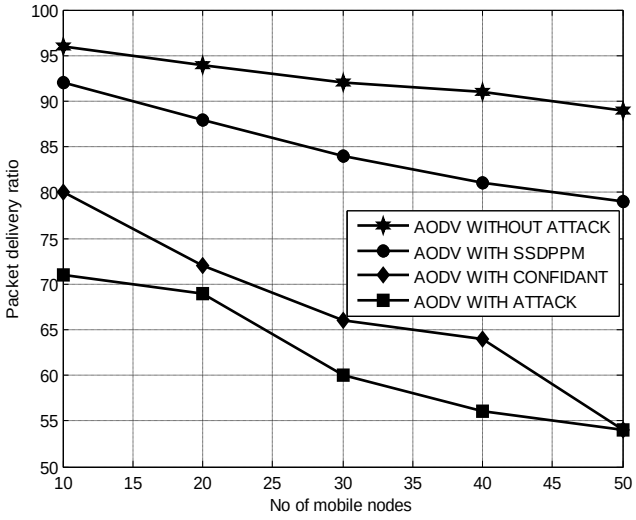

Fig.5. Performance Assessment Chart for SSDPPM based on Packet Delivery Ratio

The performance assessment of the proposed SSDPPM is analyzed by deriving throughput of the network in the above mentioned three difference scenarios. The Fig.6 illustrates the plots depicting throughput values obtained through AODV with SSDPPM, AODV with CONFIDANT, AODV with attack and AODV without attack.

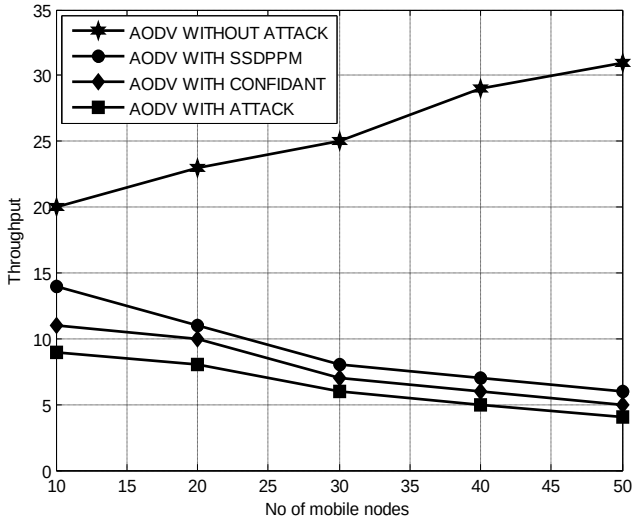

Fig.6. Performance Assessment Chart for SSDPPM based on Throughput

The proposed SSDPPM shows considerable increase in the throughput of the entire network from 6% to 12 % over AODV with CONFIDANT and 8% to 15% over AODV with ATTACK. From the results, it is clear that the proposed SSDPPM approach mitigates the attacker nodes present in that ad hoc environment in a rapid manner and increases the throughput to the average value of 7%.

The performance of SSDPPM is further studied by deriving the values of total overhead of the network environment. The following Fig.7 shows the plots of total overhead values derived from all the three scenarios viz., AODV with SSDPPM, AODV with CONFIDANT, AODV WITH ATTACK and AODV WITHOUT ATTACK. The proposed approach AODV WITH SSDPPM significantly decreases the total overhead of the network at the rate from 3% to 6% over AODV with CONFIDANT and from 10% to 17% over AODV WITH ATTACK.

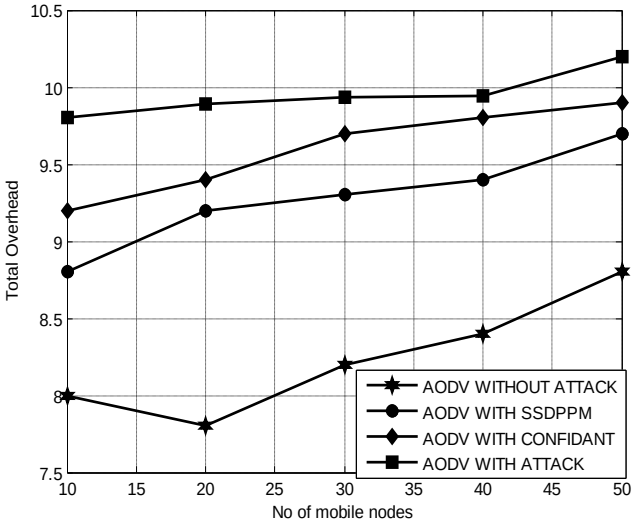

Fig.7. Performance Assessment Chart for SSDPPM based on Total Overhead

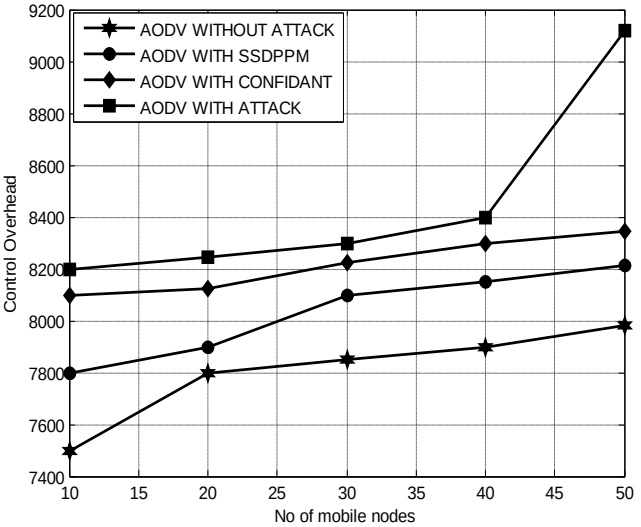

Fig.8. Performance Assessment Chart for SSDPPM based on Control Overhead

Moreover, the proposed SSDPPM approach reduces the total overhead at the average rate of 16% by mitigating the attackers nodes present in the routing path.

Finally, the performance assessment of the proposed SSDPPM is analyzed by means of measuring control overhead values of the ad hoc environment. The Fig.8 illustrates the plots depicting the control overhead values derived from all the three scenarios. The proposed SSDPPM approach decreases the control overhead of the network at the rate from 3% to 12% over AODV WITH CONFIDANT and from 6% and 17% over MAODV WITH ATTACK.

Hence, it is clear that the proposed SSDPPM approach mitigates the attacker nodes in the rapid manner and reduces the control overhead rate of the network to an average value of 14%.

6. CONCLUSION

In this paper, a secure service discovery based on probe packet mechanism (SSDPPM) has been proposed for MANETs, which is a distributed algorithm for mitigating DoS attack and thus by enhances the degree of service discovery. Further, the superior performance of the SSDPPM is analyzed based on packet delivery rate, total overhead, Control overhead and Throughput through network simulator ns-2.26. The simulation based investigation proves better results than the CONFIDANT protocol in an average by 23% and 19% in terms of packet delivery ratio and throughput. In the near future, Cohen's kappa Coefficient may be evolved to evaluate the genuineness through the probe packet mechanism designed through the fault tolerant methodology for mitigating the malicious nodes from the routing path between the source and the destination.

REFERENCES

[1] Alessandro Mei and Julinda Stefa, "Give 2Get: Forwarding in Social Mobile wireless networks of selfish Individual", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 4, pp. 569-581, 2012.

[2] P. Michiardi and R. Molva, "CORE: A collaborative repudiation mechanism to enforce node cooperating in mobile ad hoc networks", *Proceeding of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, pp. 107-121, 2002.

[3] Sonja Buchegger and Jean - Y ves Le Boudec, "A Robust Repudiation system for mobile ad-hoc networks", EPFL IC Technical Report IC/2003/05, pp. 1-11, 2003.

[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. 19-33 2008.

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

[6] Ze Li and Haiying Shen, "Game-Theoretic analysis of cooperation Incentive strategies in Mobile Ad hoc networks", *IEEE Transactions on Mobile computing*, Vol. 11, No. 8, pp. 1287-1303, 2012.

[7] Feng Li and 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, 2010.

[8] Shukor Abdul Razak, Normalia Samia and Mohd Aiziaini Maarof, "A Friend Mechanism for mobile ad hoc networks", *IEEE Computer Society International Symposium on Information Assurance and Security*, pp. 243-248, 2008.

[9] Hazer Inaltekin and 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, 2008.

[10] Joseph A. Gliem, Rosemary R. Gliem, "Calculating, Integrating , and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales", *Proceedings of Midwest Research to Practice Conference in Adult, Continuing and Community Education*, Vol. 4, pp. 82-88, 2003.

[11] Paul L. Dressel, "Some remarks on kuder-richardson reliability coefficient", *Phychometrika, Springer*, Vol. 5, No. 4, pp. 305-310, 1940.

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

[13] Chong Ho Yu, "An introduction to computing and interpreting Cronbach Coefficient Alpha in SAS", *Proceedings of the IEEE Twenty-Six Annual SAS Users Group International Conference*, pp. 246-226, 2001.