International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 6, June - 2014

Intelligent Support Vector Feed-Back based Approach for Trust Based System in Mobile Ad Hoc Network

Pawan Kumar Sharma[1]
M. Tech. Scholar ECE Dept.
SEC, SIKAR, (RAJ.)

Prof. S. C. Mahajan[2]
DEAN ECE Dept.
SEC, SIKAR, (RAJ.)

Mrs. Reena Jain[3]
Assistant Prof. ECE Dept.
SEC, SIKAR, (RAJ.)

Abstract- **A MANET, Mobile ad-hoc Network, is a collection of autonomous mobile nodes communicating over a wireless medium without requiring any pre-existing infrastructure. MANETs exhibit very interesting properties: they are self-organizing, decentralized and support mobility. The routing protocols are core concept of MANET and its offered services always face problem with resources having more time variation and are of low capacity. So it is required to make services adaptable to time variation and low capacity of resources. In this paper we are proposing an intelligent system that is capable of the selection of the routing algorithm to address a novel approach that can cope up with the network performance's degradation problem. The proposed system smartly selects new routing algorithm using an intelligent support vector feedback mechanism.**

Keywords-Manets, Routing protocol, Support vector machine, support vector classifiers**.**

I. INTRODUCTION

A. Background

Mobile ad-hoc network is a network which is independent of fixed infrastructure. It is designed for dynamically environment to exchange data among mobile nodes. Complex network situation under highly changing environment is very much suitable to MOBILE AD-HOC NETWORKS. Such complex situation includes battlefield transmission, disaster effected area, extremely remote location environment, civilian services and immediate required temporary network. Mobile nodes do not connect to a continuous power source so they face limitation of battery power and processing. Mobility nature of nodes makes them unpredictable about their joining or leaving to the networks. Due to limited range of wireless transmission among nodes, a node requires to send information from multi hop transmission. This makes routing for mobile ad-hoc network more complex to design. Routing protocol in MOBILE AD-HOC NETWORKS requires periodic advertisement broadcasted by routers. Routers collect information about their neighbourhood by sending request and response to each other. Conventional routing is not suitable for mobile ad- hoc networking. They are designed for static nodes and for less dynamic environment. Mobile ad-hoc network topologies are very dynamic so frequent re-computation of routes is required. Multi-path routing is a noteworthy requirement of mobile ad-hoc networking. It increases reliability of data transmission. It is well known that misbehavior nodes detection is very important in designing the security system for mobile ad-hoc network. It generally includes packet dropping, false routing of packets and false request in the MAC layer. Most of the time the detection techniques depend on the pre-defined threshold. Sometimes misbehavior of nodes is not caused by attacker nodes and can be due to the change in mobility of environment. In mobile ad-hoc network, when nodes want to send data to other nodes they find out the optimum path towards the destination. Suppose when a path is broken or no longer available then path finding process is required to be restarted. Mobile ad hoc networks (MANETs) are made of the collection of wireless mobile nodes which dynamically transfer data among themselves without the reliance on a fixed base station or a wired backbone network.

Mobile ad-hoc Networks have achievable use in a wide variety of situations. Such situations include moving combat zone transmissions to disposable sensors which are dropped from high altitudes and dispersed on the ground for hazardous materials detection. Civilian services include simple scenarios such as people at a conference in a hotel use their laptops with a temporary MOBILE AD-HOC NETWORKS. In case of complicated scenarios such as highly mobile vehicles on the highway which form an ad-hoc network in order to provide vehicular traffic management. MOBILE AD-HOC NETWORK'S nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility [1]. In such networks, the wireless mobile nodes may dynamically enter into the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually required for a node to exchange information with any other node in the network. Thus routing is a crucial issue to the design of a MOBILE AD-HOC NETWORKS. Routing protocols in

conventional wired networks are usually based upon either distance vector or link state routing algorithms. Both of these algorithms require periodic routing advertisements to be broadcasted by each router [2]. In distance vector routing, each router broadcasts to all its neighboring routers, in view of the changes in distance to all other nodes. The neighboring routers then compute the shortest path to every node. In link-state routing, ever router starts broadcasting to its neighboring nodes its view of the status of each of its adjacent links. The neighboring routers then compute the shortest distance to each node based upon the complete topology of the network. These old-fashioned routing algorithms are clearly not efficient for the type of dynamic changes which may occur in an ad-hoc network. In conventional networks, routers do not generally move around and rarely go away or reach the network. In a surroundings with mobile nodes, the changing topology will not only trigger frequent re-computation of routes but the overall convergence to stable routes may be infeasible due to its high-level of mobility. Clearly, routing in Mobile ad-hoc Networks must take into consideration of their important characteristics such as node mobility. Work on single path (or unipath) routing in Mobile ad-hoc Networks has been proposed. We specifically examine the issues of multipath routing in Mobile ad-hoc Networks. Multipath routing allows the establishment of multiple paths between a single source and single destination node. Multipath routing is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing. Load balancing is of special importance in Mobile ad-hoc Networks due to limited bandwidth between the nodes.Mobile ad hoc networks are self-ruling systems of mobile hosts connected by wireless links. This sort of networks are getting more and more importance due to variety of services offered, such as personal networks of Laptops and PDA's (Personal Digital Assistants), military services, civil services and emergency operations. To achieve efficient transmission between nodes connected to the network various routing protocols are available. A mobile ad hoc network is a concept that has received a large attention in scientific research. It includes mobile routers (and associated hosts) connected by wireless links. The routers are free to be in motion randomly and systematize themselves accordingly; thus, the network's wireless topology may change rapidly and suddenly. Such networks may operate in a separate fashion, or may be connected to the larger Internet. Mobile ad-hoc Networks are useful in many services and for such services they do not require any infrastructure support. There are many routing protocols which have been developed for mobile ad-hoc networks. For example, Ad-hoc on-demand Distance Vector Routing (AODV) is one such widely used lightweight routing protocol. The main function of a routing algorithm is to find an initial path between a source and a destination, and then maintain data forwarding between two nodes. Destination-Sequenced Distance-Vector Routing (DSDV) protocol uses the Bellman–Ford algorithm to calculate the path. The cost metric is used in the hop count which is the number of hops it takes for the packet to reach its destination. DSDV is a table driven proactive protocol. Thus, it maintains a routing table for all the nodes in the entire network and not for just the neighbors of nodes.

B. Trust Based System

It is well known fact that MANETs (Mobile ad-hoc Networks) are extremely vulnerable to a diversity of attacks, and customary security mechanism does not work well for them. Many security schemes have been projected that depend on collaboration amongst the nodes in a MOBILE AD-HOC NETWORKS for identify nodes that exhibit attacker behaviors such as packet dropping, modification, and misrouting. We argue that in general, this trouble can be viewed as an example of detecting nodes whose behavior is an outlier when compared to others. A Mobile Ad-hoc Network, as its name says, is normally composed of a dynamic set of supportive nodes that are willing to relay packets for other nodes due to the lack of any pre-implemented network infrastructure. Mobile Ad-hoc networks (MANETs) have a variety of civilian and armed forces services, ranging from disaster rescue, personnel coordinating efforts after a storm, tremor or fire incident to soldiers exchanging information for situational awareness on the battlefield. Other probable services include personal and house area networking, real-time traffic alert propagation via vehicular networks. Several factors make Mobile ad-hoc Networks very vulnerable to various misbehaviors such as intrusions. First of all, data in Mobile ad-hoc Networks is transmitted via Radio Frequency broadcasts, which can be easily eavesdropped on or even modified. Second, nodes in Mobile ad-hoc Networks have restricted power supply, and as a result their performance is severely tainted when power is finished. Third, when they are used for safety and armed forces purposes, nodes in Mobile ad-hoc Networks are susceptible to cooperation and manipulation by adversaries. Hence, it is obvious that misbehavior discovery should be a crucial component of any security solution that aims to defend the mobile ad hoc networks. The misbehavior classically observed includes dropping of packets, misroutes, bogus Requests/Clears in the MAC layer. However, many of these actions can also happen due to ecological and mobility related reasons, not just attacker intention. Most of the current misconduct detection mechanisms rely on a predefined threshold to make a decision if a node's behavior is attacker or not. However, it is rather hard to set a suitable threshold due to the reason that the network is pretty dynamic and random. In contrast, they are not supposed to rely on any previous information to find a node that is an outlier with respect to a given evident. From the given information that an attacker node generally behaves in a different way when compared to other nodes, we can detect the node's misbehavior by means of outlier discovery. Besides misconduct detection, trust management is another well-studied technique that can be used to safe Mobile ad-hoc Networks. The main reason of trust management is to calculate the behaviors of other nodes, and thus build a status for each node based on the result of behavioral assessment. Most of the trust management schemes in Mobile ad-hoc Networks are proposed and the

honesty of a node in one dimension, i.e., all observations are used to compute a single scalar trust for each node. However, a single trust metric may not be communicative enough to sufficiently explain whether a node is reliable or not in many complex scenarios.

II. RELATED WORK

In the literature there are so many research have been presented on multipath routing [1-2]. Wenjia Li et al. [3] have proposed a SVM-based Misbehavior Detection and Trust Management framework (SMART) is described to address the security threats caused by various misbehaviors. In SMART, the Support Vector Machine algorithm is used to detect node misbehaviors, which does not require any pre-defined threshold to distinguish misbehaviors from normal behaviors.

Wenjia li and Anupam Joshi [4**]** have proposed a multidimensional trust management approach to cope with nodes misbehaviors in Ad-Hoc networks Various trust management schemes have been studied to assess the behaviors of nodes so as to detect and mitigate node misbehaviors in MANETs.. A multi-dimensional framework to evaluate the trustworthiness of MANET node from multiple perspectives is defined. The scheme evaluates trustworthiness from three perspectives: collaboration trust, behavioral trust, and reference trust.

A.Pravin Renold and R.Parthasarathy [5] have proposed an approach based upon trust to provide security to Ad hoc On-demand Distance Vector (AODV) protocol, which helps AODV to detect the compromised nodes.

Profit of Multipath routing as mentioned before, multiple paths can provide load balancing, fault-tolerance, and higher aggregate bandwidth. Load balancing can be achieved by spreading the traffic along multiple routes. This can improve congestion and bottlenecks. From a fault tolerance perspective, multi-path routing can present route resilience. To demonstrate this, consider Figure

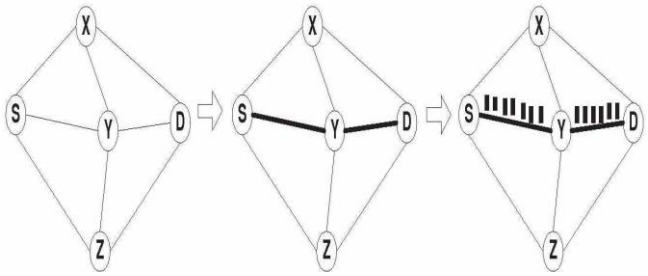

Fig 1. An example of route discovery in an ad hoc network Source: [2]

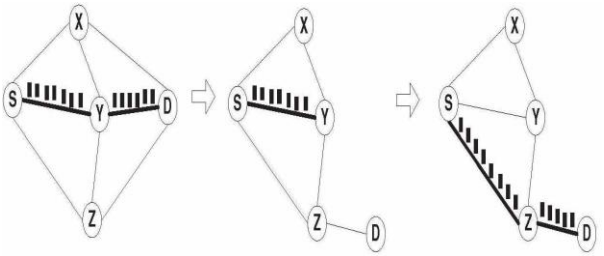

Fig 2. An example of route maintenance in an ad hoc network Source: [2]

Where node S has established three paths to node D. If node S sends the same packet along all three paths, as long as at least one of the paths does not fail, node D will receive the packet. While routing redundant packets is not the only way to utilize multi-path paths, it demonstrates how multi-path routing can provide fault tolerance in the presence of route failures. Since bandwidth may be limited in a wireless network, routing along a single path may not provide enough bandwidth for a connection. However, if multi-path paths are used simultaneously to route data, the aggregate bandwidth of the paths may satisfy the bandwidth requirement of the services. Due to nodes in the network communicate through the wireless medium; radio interference must be taken into account. Transmissions from a node along one path may interfere with transmissions from a node along another path, thereby limiting the achievable throughput. However, results show that using multi-path routing in ad hoc networks of high density results in better throughput than using unipath routing [2]

III. METHODOLOGY AND RESEARCH ISSUES & CHALLENGES

A. Challenge Identification

. Mobile ad-hoc Networks are becoming useful due to the existing wireless infrastructure is costly and not convenient now a days. MOBILE AD-HOC NETWORKS is becoming important part of next generation mobile services. The mobile nodes must co-operate at the routing level in order to forward packets to moderate the behavior in MOBILE AD-HOC NETWORKS. It is required to build the relationship between the mobile nodes in the MOBILE AD-HOC NETWORKS and select routes based on the trust. A dynamic feedback mechanism should be designed in which mobile nodes monitor the behavior of their neighbors and exchange information about other nodes in the MOBILE AD-HOC NETWORKS.

In Mobile ad-hoc network, nodes communicate with each other through wireless mode. Neighbor nodes are those nodes which come under the wireless range of the other. Due to rapid changing topology, mobile nodes randomly join and leave the network. Nodes generally send data to neighbor nodes. When data is sent to a destination nodes and detonation nodes is a neighbor node then data exchange is done very easily. But normally target node is non neighbor node so data is send through a series of multiple hops, with intermediary nodes. Mobile ad –hoc

network has various issues and one of them is unpredictable environment. MOBILE AD-HOC NETWORKS thus designed for unknown situation where infrastructure based network setup is very complex. Nodes require some resource prerequisite for transfer such as user related data, location, network information. Thus effective transmission among nodes is very much required aspect of mobile ad-hoc network. Since we know that the network is affected by various situations such as route expiration, misrouting of information and non optimized path towards detonation. An optimized path selection is now a days a very interesting topic among researchers. There are various protocol defined to overcome the non optimized path challenge.

B. *Methodology Used*

Mobile ad-hoc network's offered services always face challenge with resources having more time variation and low capacity. As a result, the service quality that a service requires depends on the quality of the network. This network quality should cooperate with the available resources in the wireless medium and in the mobile nodes in the network as well. Stability of resources is also very important factor while providing services. It is also required to build the relationship among the nodes. Selection of best routes should be decided on the basis of a trust among the mobile nodes. Forwarding data among nodes without any verification of destination will create many challenges. To identify of these challenges a better approach is required to provide a best path and selection of new routing mechanism. There are various mechanisms available to provide better support vector classifier in mobile ad-hoc networks but still there is lot of scope available in improvement of the support vector classifier propagation in mobile ad-hoc networks.

We are proposing an intelligent system that is capable of the selection of the routing approach to address a novel approach that can cope with the network performance's degradation challenge. The proposed system smartly selects the best routing algorithm using an intelligence support vector feedback mechanism according to the networking perspective. Support vector feedback method is helpful into analyze the node's behavior in mobile ad-hoc networks. Routes are selected on the basis of trust relationship between the mobile nodes in the mobile ad-hoc networks. The parameters selected to describe the networking perspective are the network size and average mobility. The proposed system functions by reliable routing mechanism with the time to keep the network performance at the best level. The parameters selected to describe the network context are the network size and standard mobility. The planned system then function by changeable the routing mechanism with the time to keep the network performance at the most effective level. The chosen algorithm has been exposed to produce a combination of higher throughput; average delay, packet delivery fraction, and packet loss. Hence, it is helpful to provide best approaches support vector in mobile ad-hoc networks. We have used NS-2 as a simulation environment and the support vector classifiers are used to find best and most trusted path for proposed routing algorithm.

IV. PROPOSED SOLUTION

A. *Proposed System*

In this research work we have focused on finding best path for destination. Path detection process requires selecting nodes having better trust value as compared to other nodes. We have presented a dynamic trust mechanism using a support vector machine classifier. Simulation results show that our approach has improved network performance.

Our proposed system requires a network simulator to perform the simulation of mobile nodes in order find the best routing approach to improve the performance of MOBILE AD-HOC NETWORKS. Network Simulator (NS-2) has been used to perform simulation.

B. *Feedback Based Route Selection Using Svm Classifier*

Our proposed system select the optimum route to provide an approach that enhance network performance. Our system uses an intelligent protocol that uses an SVM based intelligence feedback mechanism that uses a intelligent feedback method. This system is trying to analyze the node's behavior in MOBILE AD-HOC NETWORKS. When a node generates a path to transmit the data to target nodes and it is found a sudden broken path then it selects alternative path and forwards the data. SVM is used as the classifier to classify the nodes trust while forwarding the packet from one location to another location. As we know SVM can tackle the classification challenge successfully hence a classification approach includes training and testing of data sets. These data sets are fetched from the various network parameters such as packet forwarding and dropping ratios. Each example in the training set includes one target value and several attributes.

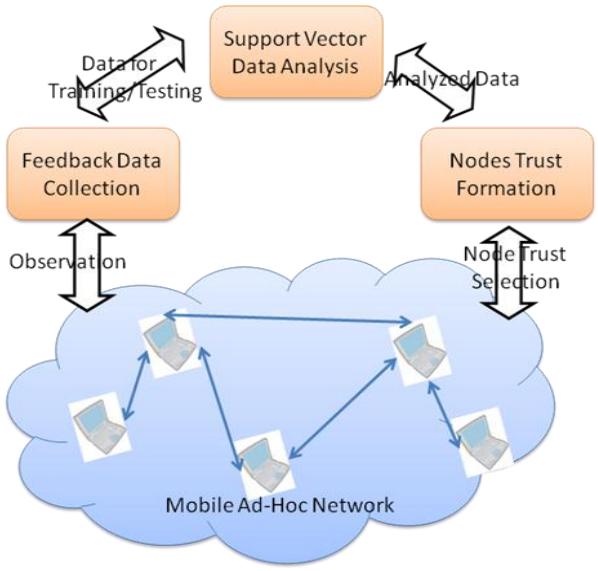

Fig 3. Intelligent Feedback Support Vector Classification System

SVM model is designed to predict the target values of the data examples in the testing set. The testing set is generally provided by the network traffic that is under observation. Our works follow the routes configuration plan in which routes are selected on the basis of trust relationship among the mobile nodes in the MOBILE AD-HOC NETWORKS. The parameters selected to describe the networking perspective are the network size and average mobility. Our proposed system functions enhance performance by using reliable routing mechanism. The parameters that are used to describe network performance are size, packet loss, average delay, link failure and average mobility. In our approach we have calculated trust value of neighbor node after a periodic interval at each and every node.

To calculate trust value of a node we have used support vectors. SVM takes raw data as input of various dimensions and after data collection it performs scaling of data and then it classifies the data into various categories. In this work we have selected two categories normal and trusted. Packet forwarding, packet delay, packet drop, link failure, link expiration time, source node and destination node are taken as feature sets for support vector approach.

After calculating the trust value of neighbor node using SVM this value is updated to every node before each packets forwarding. Trust value is generated for every nodes and it is updated after periodic intervals. This trust value is helpful in deciding routing path to destination. Our approach provides the trust based path finding system. Trust value environment is updated at nearest neighbor node and the periodic interval is reset after the link is broken. In this work, we are splitting the communication between source and destination into two neighbor nodes. It is helpful in the situation where a link is broken or node is moved to some other location. This approach does not start rerouting process from the source node but it starts alternate path request from the node where link was broken found. Thus the end to end delay is controlled.

Whenever a packet is generated, the packet generating node finds a nearest node towards destination based upon trust value of that particular nearest node with satisfying conditions as defined in MANET routing algorithms. Here the flow graph is showing the path formation using SVM support vector classifiers.

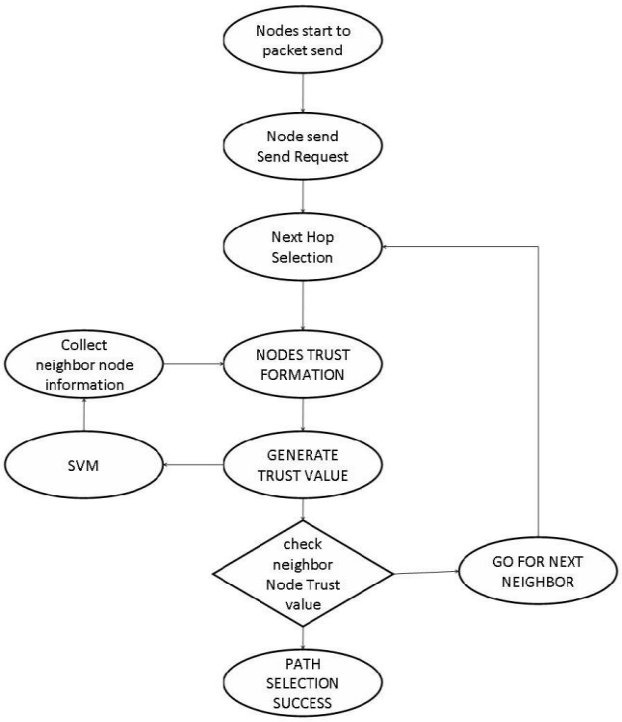

Fig 4. Path formation using SVM

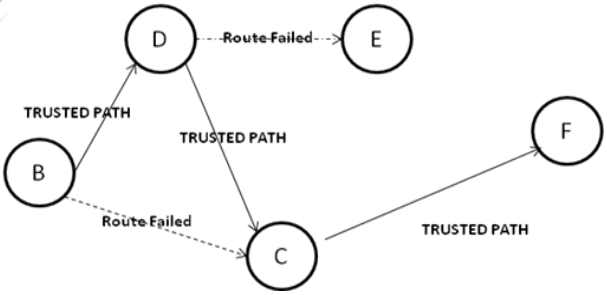

Fig 5. Best trusted optimized route scenario 1

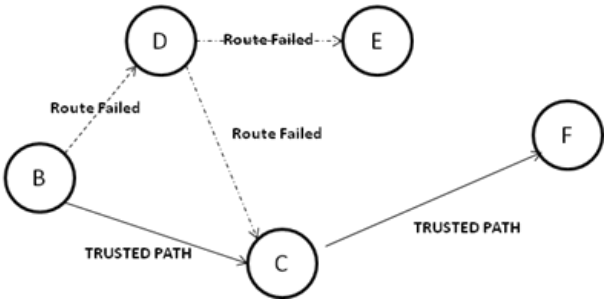

Fig 6. Best trusted optimized route scenario 2

In our research work, we have developed an intelligent system that is capable of the selection of the routing algorithms to address a novel approach that can cope with the network performance's degradation challenge. For the proposed system, we have developed a routing algorithm

that uses an intelligence feedback mechanism according to the networking perspective.

V. RESULT AND ANALYSIS

TABLE 1. Simulation Parameter

S. No.	Parameter	Value
1	Number of nodes	100
2	Simulation time	100 sec
3	Simulation Model	Two Ray Ground
4	MAC Type	802.11
5	Link Layer Type	LL
6	Interface Type	Queue
7	Traffic Type	CBR
8	Packet Size	512 byte
9	Queue Length	50
10	Node Speed	20 m/sec

A. *Performance Evolutions*

We evaluate the performance of the proposed mechanism using the Network Simulator NS-2 and compare it to the AODV and DSDV protocol. We have simulated a wireless ad hoc network area with the size of 700 m * 700 m. In this evaluation, we have focused on data packet loss, packet delivery fraction, and average end to end delay of the network to measure the network performance.

Packet delivery fraction (Pdf.) : it is defined as the ratio of the number of packets successfully delivered to the destination to those generated by the source.

$$\text{Pdf} = \frac{\text{Received Packets}}{\text{Sent Packets}} \times 100$$

Average End- to- End delay: it is the average time taken by data packets to move from source to destination across the MANETS. [6]

Simulation result shows that our proposed approach outcome is better than the existing mobile ad-hoc network protocol.

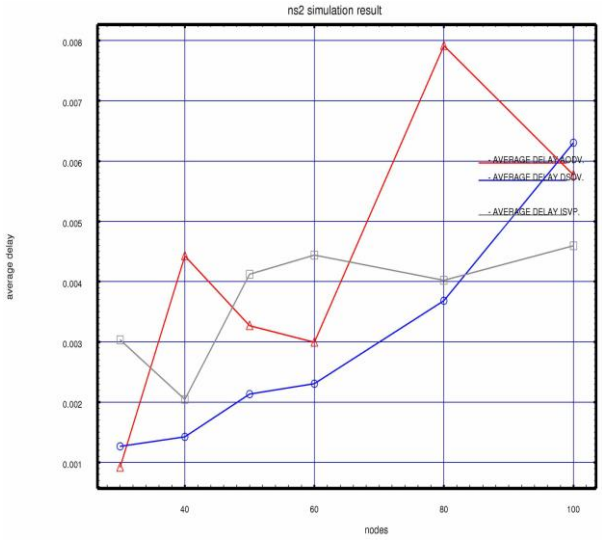

Fig 7. Average delay vs. nodes

TABLE 2. Comparison of Average Delay

Nodes	DSDV	AODV	ISVP
30	0.00126	0.00091	0.00303
40	0.00142	0.00442	0.00204
50	0.00823	0.00326	0.00412
60	0.00230	0.00299	0.00444
80	0.00368	0.00791	0.00402
100	0.00630	0.00577	0.00459

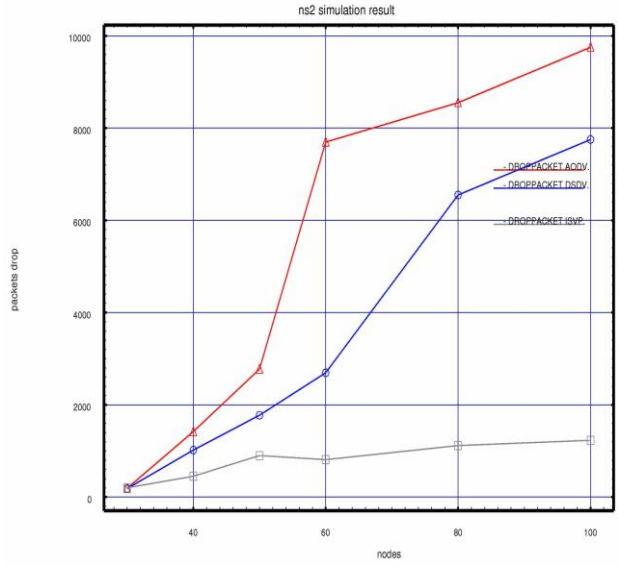

Fig 8. Packet drop vs. Nodes

TABLE 3. Comparison of Packet Drop

Nodes	DSDV	AODV	ISVP
30	185	190	202
40	1019	1419	451
50	1774	2774	900
60	2696	7696	812
80	6550	8550	1117
100	7752	9752	1231

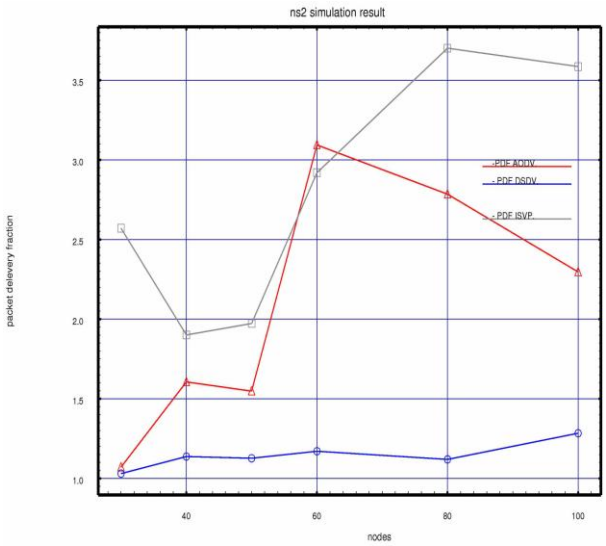

Fig 9. Packet delivery fraction vs. nodes

TABLE 4. Comparison of Packet Delivery Fraction

Nodes	DSDV	AODV	ISVP
30	1.02982	1.07006	2.57039
40	1.13663	1.60542	1.9006
50	1.12611	1.54742	1.9725
60	1.17038	3.09332	2.9186
80	1.11916	2.78436	3.70073
100	1.28323	2.29587	3.58276

VI. CONCLUSION

Our system is able to select of the routing algorithm based on intelligent support vector feedback which improves the performance of the network. The system work is focuses on support vector feedback mechanism which is best in its class due to the fact that it avoids the path selection randomly. It maintains the best routing path on the basis of trust based relationship among the nodes. The parameters selected to describe the networking perspective are the network size and average mobility. The proposed system functions by reliable routing mechanism with the time to keep the network performance at its best level..

The silent features of the proposed system are:

- Our proposed intelligent system will address the selection of the desired routing algorithm that will improve the performance in order to provide more effective support vector classifier among the mobile nodes of MOBILE AD-HOC NETWORKS.
- It also provides reliable routing approach which will be helpful in finding the best path before the process starts.
- The proposed system will vary the routing mechanism with the time to keep the network performance at the best level produce higher throughput; average delay, packet delivery fraction and packet loss in mobile ad-hoc networks.

REFRENCES

[1] Lipika Rajanandini Sahu & Sankarsan Sahoo " Issues and Performance Measurement of Routing Protocols in MANET :An Empirical study" International Conference on Recent Innovations in Engineering & Technology, ISBN : 978-93-83060-46-7,19-20 April 2014, GITA, BBSR

[2] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges" in Performance Tools and Services to Networked Systems Computer Science Volume 2965, 2004, pp 209-234 ISBN 978-3-540-24663-3

[3] Wenjia Li, Anupam Joshi, Tim Finin, "SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks", IEEE Transactions on Dependable and Secure Computing 18 DEC 2010.

[4] A.Pravin Renold and R Parthasarthy " Source Based Trusted AODV routing protocol for mobile Ad-Hoc Networks" ICACCI'12 Aug 3-5 2012 chennai T Nadu India .

[5] The Network Simulator ns-2. [Online; accessed February 20th, 2011]. Available at: http://www.isi.edu/nsnam/ns/

[6] Akshai agrawal,savita Gandhi and nirbhay chaubey "PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETs" international journal of distributed and parallel system Vol.2 No.6 Nov.2011

[7] A.Makolo " Support vector Machine for improving performance of TCP on hybrid network" in African journal of computing & ICT Vol5 No 6 dec2012 ISSN 2006-1781

[8] Xin li , Zhiping jia , Haiyang wang, and luguang wang " Trusted based on demand Multipath Routing in Mobile Ad- Hoc network" in journal IET Information Security 20 dec 2010.

[9] Ms. K. Deepa and Mrs. V Durgadevi " Secured Routing For Manet using friend based Ad-hoc routing (FAR) " in International Journal of Innovative Research in Computer and Communication Engineering VOL 2 ISSUE 1 March 2014 ISSN 2320-9798.

[10] Zheng Yan Peng Zhang Teemupekka Virtanen "trust evolution Based security solution in Ad-hoc networks " article published in Nokia research centre Nokia group Helsinki Finland 2003.

[11] Bartosz Biskupska ,jim dowling and Jan Sacha " Properties and Mechanisms of self organizing MANET and P2P systems" ACM Transactions on Autonomous and Adaptive Systems, Vol. 2, No. 1, Article 1, Publication date: March 2007

[12] Jim dowling Eoin curran Raymond Cunningham and vinny cahill " using Feed back in collaborative Learing to Adaptively optimize MANET Routing " IEEE TRANSACTIONS ON SYSTEMS,MAN AND CYBERNETICS PART A SYSTEMS AND HUMANS VOL.35 NO.3 MAY 2005.

[13] M.Kartik and K. Venkateswara " ALIX Route Optimization Mechanism in MANET'S For AODV " international journal of computer Technology and applications VOL 3(6) 2073- 2076 ISSN 2229-6093.