International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Intelligent Feedback Support Vector Classification System for Best Path Discovery in Mobile Ad Hoc Network

Sheetal Jaiswal[1] , Shraddha Kumar[2]
[1, 2.] Department Of Computer Science & Engineering
S.D. Bansal College Of Technology
Indore, India

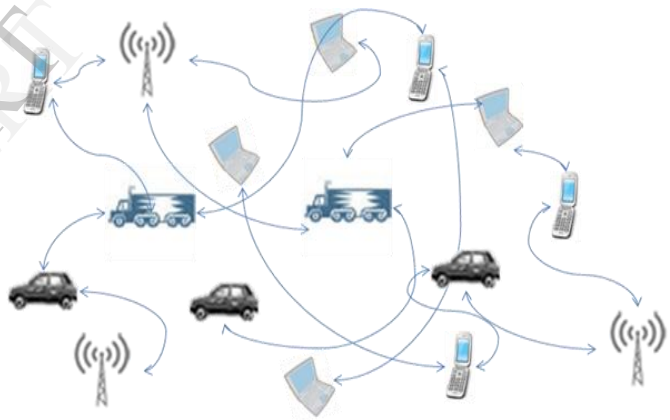
***Abstract*: MANET is a group of wireless nodes that can dynamically form a network to exchange information without using fixed network infrastructure. As we know that setup a new network is a costly and non convenient task. Here MANET comes into the picture, it has capability to be setup easily and not too expensive. A network also requires costly and complex component while being established. Mobile ad-hoc network can be setup using any device supporting basic wireless facility. Since this network is easy to be setup and does not require any specific support so it is very popular among users. Nodes need to forward data among each other by using routing protocol. These protocol is designed to select best path to provide communication. Nodes in mobile ad-hoc network are required to select trusted node from their neighbor. In this approach we have describe an approach to find the trusted nodes into MANET and select the path from these trusted node to provide better trusted path. We have developed a mechanism to monitor the behavior of their neighbors and exchange information about other nodes. Our system is able to select the optimized route to reduce the network performance's degradation problem. The proposed system selects the best routing protocol using an intelligence support vector classification feedback mechanism according to the networking requirement. We have given tested set to our classifier to judge the nodes behavior and find the trusted node in selection of path. We have perform simulation and compare our approach to other exiting protocol and it is proved that our approach is improving the network performance.**

Key words— Mobile Ad-hoc network, Routing protocols, Trust establishment, Support Vector, Classification.

I. INTRODUCTION

Mobile ad-hoc network is a network 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 MANET environment. Such complex situation includes battlefield communication, disaster effected area, very remote location environment, civilian applications 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 needs to send information from multi hop communication. This makes routing for mobile ad-hoc network more complex to design. Routing protocol in MANET require periodic advertisement broadcast by routers. Routers collect information about their neighbor by sending request and response to each other. Conventional routing is not suitable for mobile ad hoc networking.

Fig 1: Mobile Ad-hoc Network environment



They are designed for static nodes and less dynamic environment. Mobile ad-hoc network topologies are very dynamic so frequent re computation of routes is required. Multipath routing is 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 these detection techniques depends on the predefined threshold. Sometimes misbehave of nodes is not by malicious nodes but because of mobility environment changes. In mobile ad-hoc network, when nodes want to send data to other nodes. it needs to find out the optimum path towards to destination. Suppose when a path is broken or no longer available then path finding process is required to restart. In this paper we focus on finding best path for destination. Path detection process requires selecting nodes having better trust value compare to other nodes. We have presented a dynamic trust mechanism using a support

vector machine classifier. Simulation shows that our approach has improved network performance.

II. Routing in Mobile Ad Hoc Networks:Issues and Challenges

A mobile ad hoc network (MANETs) is collection of wireless mobile nodes which exchange data without fixed base stations. Nodes are naturally have very limited power, processing, and memory resources and high level of movement. In MANET, the wireless mobile nodes can enter the network and leave the network anytime without any restriction. Multiple hops are usually required for a node to trade information with any other node in the network due to the limited transmission range. Authors' examine the issue of multipath routing in MANETs [1]. A single source and single destination node can form multiple paths in multipath routing. The reliability of data transmission is enhanced according to authors in their approach. Load balancing among the various nodes is enhanced in the approach because it is very important factor due to limited bandwidth [4]. In proposed work authors

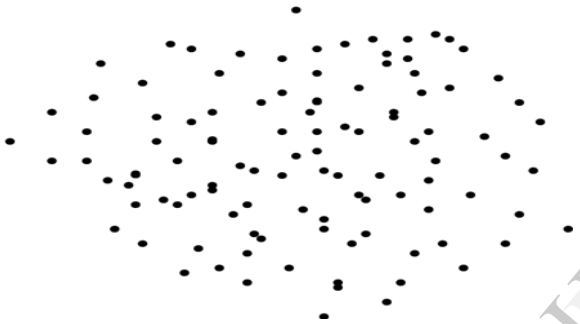


Fig 2: Mobile nodes in action in simulation of MANET

verify that by using multipath routing in existing approach reliability, load-balancing, energy-conservation, and Quality-of-Service of system is enhanced [8][9].

MANET is not dependent on the pre existing infrastructure. It leads to requirement to transmit packet among nodes for the nodes those are not in the communication range. Multi hop communication is the need of mobile ad-hoc network due to limited range and frequent movement of nodes. Authors discuss the selfish and malicious nodes that denied the cooperation in network. Sometimes these nodes attempt to interrupt the services [6][7]. The proposed system, SVM based detection system is focuses on security violation caused by malicious nodes. Authors proposed approach described an algorithm to classify these modes misbehavior. SMART does not require any given threshold to distinguish the normal versus misbehavior nodes. MANET nodes trustworthiness is calculated by multi dimensional trust management model. This model defined nodes trust from multiple perspectives into more accurate and effective manner. A deep study is done by author's by simulation to validate SMART framework and it shows that it is better than previous schemes. Node's high mobility adversaries are handled by proposed framework [9].

Security in mobile ad-hoc network is very crucial topic for researchers. There is lot of research work going on to provide secure communication in MANET. Security is divides as general into many categories. Open transmission medium is largely used in MANET [2][3]. The open transmission makes eavesdropping easier. As we know, MANET works in the absence of any fixed infrastructure so cooperation among the nodes becomes important ant features from security. The MANET security must be more robust to handle various type of security breaches. Mobile nodes in MANET are not able to obtain a global view of network due to short transmission range and limited battery. it leads to further cooperation among nodes is more important to get the idea what is happening among nodes in whole network. mobile node communication is interrupted due to high mobility and random movement of nodes from time to time in the network.

The support vector machine is useful in recognizing in misbehavior in node's communication. by using SVM classifier we can separate nodes which is misbehaving in network. Smart framework uses SVM classifier to determine misbehaving nodes without declaring any pre determined threshold. This will remove complication in detecting in complicated scenario where network is changing very randomly [2][9].

Authors discuss mobile nodes trustworthiness into many aspect and deployed multidimensional trust management scheme. A node's trust is decided on various parameter such as cooperation among nodes, abnormal behavior of nodes and honesty in data forwarding. Nodes trustworthiness is adjusted acceding to the attributes of behavior done by nodes in the context of their appearance.

It is well known that mobile ad-hoc network is very dynamic in nature so very much prone to various attacks and conventional solution is not very effective. For misbehavior nodes identification depend on cooperation between nodes. these process consist of analyzing malicious behavior, packet dropping, packet modification, and packet misrouting [7][10]. Detection of nodes whose behavior is susceptible compare to other nodes. A collaborative and trust based detection scheme is proposed that focuses on various aspects and separate misbehaved nodes from normal nodes with a limited communication range.

MANET routing protocol usually discover routes by sending request packets into entire network. This process normally creates more overhead into network. NARD approach discusses neighbor assisted route discovery protocol for mobile ad-hoc network. A limited portion of network is affected. source node sends control packet to limited number of nodes. Search criteria include searching for destination neighbor nodes. NARD enhances network performance by reducing network overhead by limiting the flooding for a portion of nodes. It is seen that the approach is better than other protocols [4].

A novel middleware approach specialized for consistent and efficient wireless communication is described. Machine-learning based analysis is applied for meaningful communication by optimizing local information for current application scenario. A middleware component is defined for cooperation among the infrastructure based and ad-hoc communication. It generates communication prediction and send into network for further references. Communication prediction includes connective information of mobile nodes. Network communication performance is enhanced by

cooperation between communication layer and application layer information [1][2].

III. Issues in Designing MANET Routing Protocol

In Mobile ad-hoc network, nodes communicate to each other through wireless mode. Neighbor nodes are those nodes which comes under the wireless range of other. Due to rapid changing topology, mobile nodes randomly join and leave the network. Nodes generally send data to neighbor nodes. When data is send 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 issue such that unpredictable environment. MANET us 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 communication among nodes is very required aspect of mobile ad-hoc network. Since as we know 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 problem.

Table 1: Simulation parameters of Network Simulator

	Parameter	Value
1	Number of nodes	100
2	Simulation time	50 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 MB
9	Queue Length	50
10	Node Speed	20 m/sec

IV. Feedback 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 MANET. 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 forward the data. SVM is used as the classifier to classify the nodes trust while forwarding the packet from on location to another location. As we know SVM can tackle the classification problem successfully. 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 instance in the training set includes one target value and several attributes.

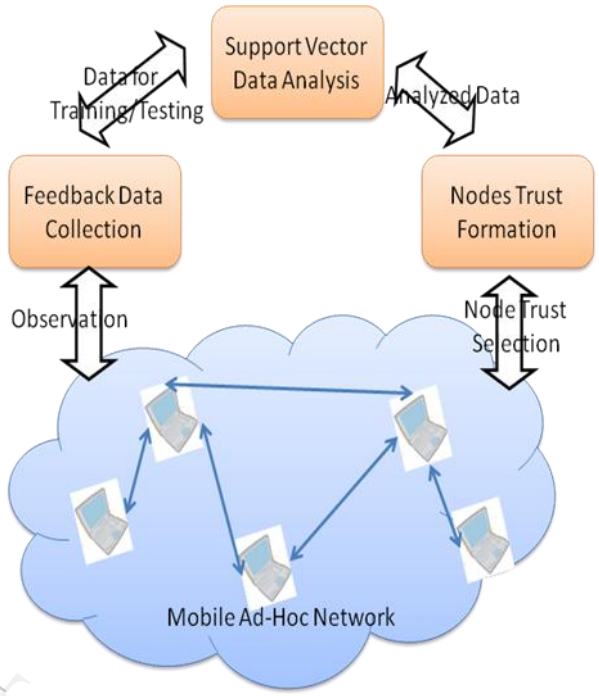


Fig 3: Intelligent Feedback Support Vector Classification System

SVM model is designed to predict the target values of the data instances 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 MANET. 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.

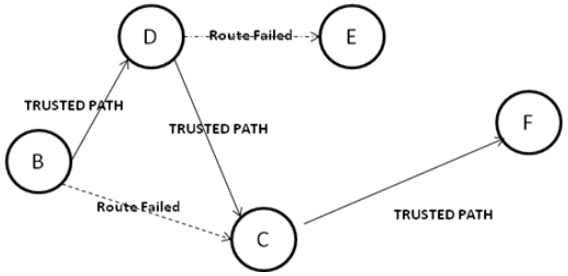


Fig 4: Best trusted optimized route scenario 1

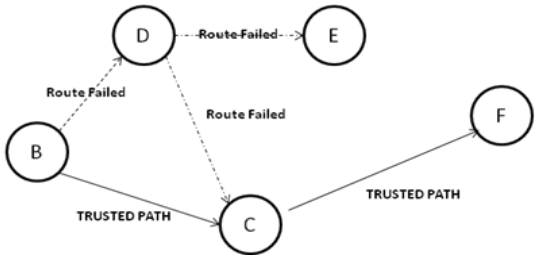


Fig 5: Best trusted optimized route scenario 2

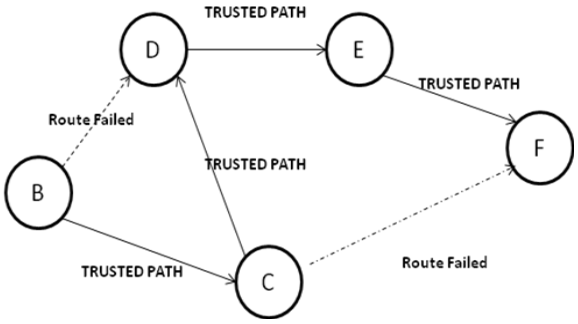


Fig 6: Best trusted optimized route scenario 3

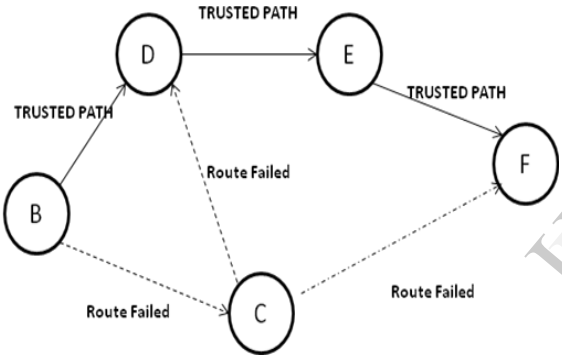
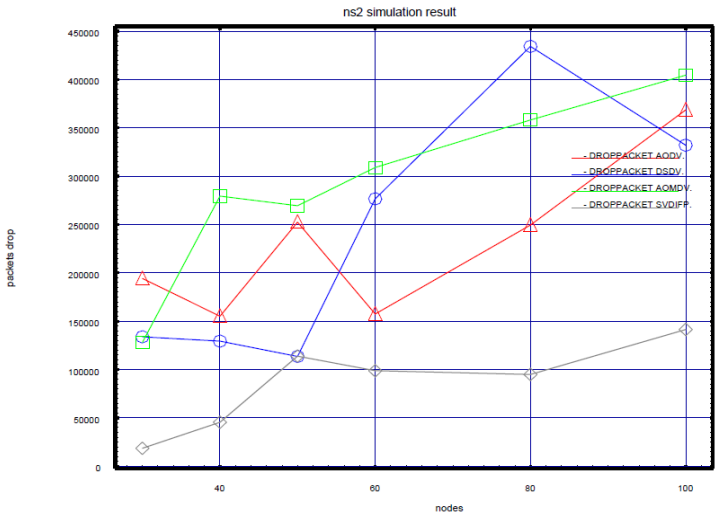


Fig 7: Best trusted optimized route scenario 4

V. Performance Analysis

We evaluate the performance of the proposed mechanism using the Network Simulator (NS-2) and compare it to the AODV and AOMDV 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, throughput and average end to end delay of the network to measure the network performance. Data packet loss is defined as the ratio of the number of packets received at the destination to the number of packets sent by the source. We also calculate the throughput which is defined as the fraction of the amount of successful packet delivery ratio to the total amount of packets. Simulation result shows that our proposed approach outcome is better than the existing mobile ad-hoc network protocol.

Fig 8: Packet drop comparison in Network



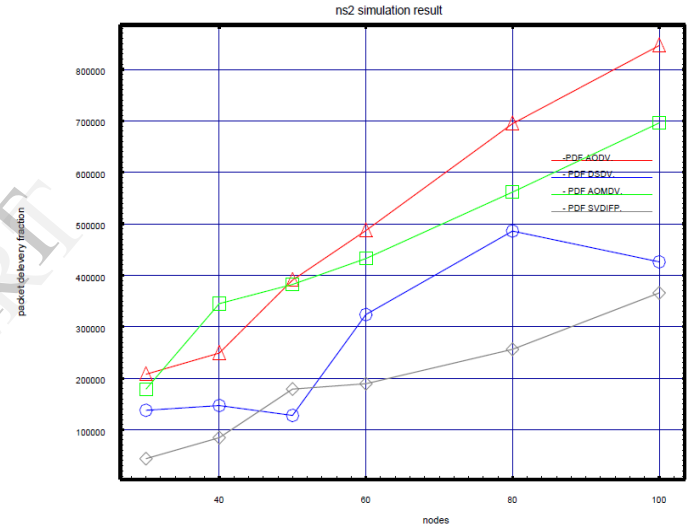


Fig 9: Successful Delivery Ratio in Network

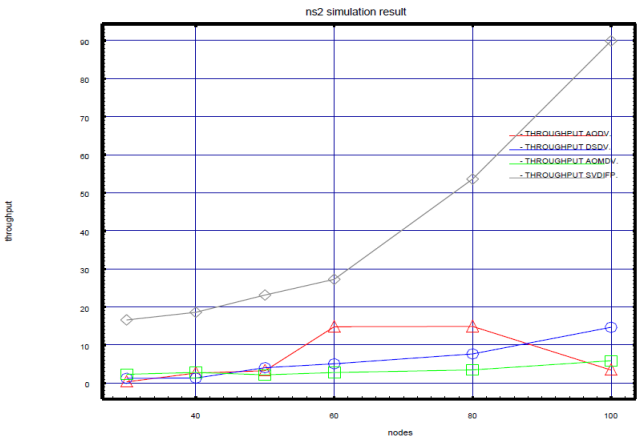


Fig 10: Throughput comparison graph in Network

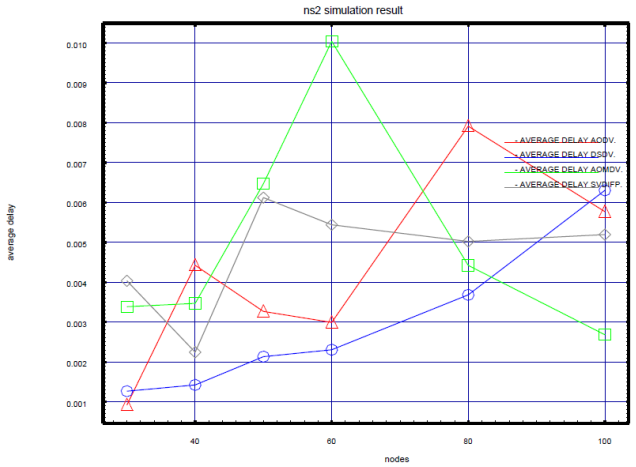


Fig 11: Average Delay comparison in Network

VI. CONCLUSION

In MANET, mobile nodes are randomly changing their position. This results into degradation into the network performance. It is required to maintain the routing parameters among all nodes. In this paper we have discussed better selection strategies of path. Node having the better trust value is selected as a next hop. Node's trust is depend on various parameter. Theses value is changing with the random movement of nodes. SVM classifier is used to select node's trust. Nodes behavior is provided as attesting set in our approach. We have gone through extensive simulation using ns2 simulator. The result shows that our approach is better than existing approach.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R. B. G.) thanks . . ." Instead, try "R. B. G. thanks". Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

REFERENCES

[1]. Jiajia Liu, Nei Kato, Senior Member, IEEE, "Generalized Two-Hop Relay for Flexible Delay Control in MANETs", IEEE/ACM TRANSACTIONS ON NETWORKING, DOI 10.1109/TNET.2012.2187923

[2]. Frank Nordemann, "A communication-optimizing Middleware for efficient wireless communication in rural environments " , Middleware 2012 Doctoral Symposium, December 3, 2012, Montreal, Quebec, Canada. 2012 ACM 978-1-4503-1611-8

[3]. Rodrigo do Carmo, Marc Werner, and Matthias Hollick, "Signs of a Bad Neighborhood: A Lightweight Metric for Anomaly Detection in Mobile Ad Hoc Networks", Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus.

[4]. J. Gomez, V. Rangel, "Neighbor-assisted route discovery in MANETs", @Springer Wireless Networks November 2011, Volume 17, Issue 8, pp 1745-1761

[5]. Zygmunt J. Haas and MilenNikolov," Towards Optimal Broadcast in Wireless Networks", MSWiM'11, October 31–November 4, 2011, Miami, Florida, USA. 2011 ACM 978-1-4503-0898.

[6]. Khabbazian, M., Bhargava, V. "Efficient Broadcasting in Mobile Ad Hoc Netorks," IEEE Trans. on Mobile Comp., Vol.8, No.2, Feb. 2009

[7]. Fenggang Wu, Hongzi Zhu, Jia-Liang Lu, "On Optimal Service Directory Selection in Urban Vehicular Networks" , UrbaNE'12, December 10, 2012, Nice, France. 2012 ACM 978-1-4503-1781.

[8]. Stephen Mueller, Rose P. Tsang and DipakGhosal , "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges" in springer Performance Tools and Applications to Networked Systems Lecture Notes in Computer Science Volume 2965, pp 209-234

[9]. Wenjia Li, Anupam Joshi, and Tim Finin, "An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks " in UMBC TECHNICAL REPORT CS-TR-11-01

[10]. Wenjia Li & James Parker &Anupam Joshi, "Security Through Collaboration and Trust in MANETs " in Springer Mobile Networks and Applications June 2012, Volume 17, Issue 3, pp 342-352

[11]. A.PravinRenold, R.Parthasarathy, "Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks", ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India., 2012 ACM 978-1-4503-1196-0.

[12]. MilenaRadenkovic, Ivan Vaghi, "Adaptive User Anonymity for Mobile Opportunistic Networks", CHANTS'12, August 22, 2012, Istanbul, Turkey.

[13]. Marwaha, S. et al.: Challenges and Recent Advances in QoS Provisioning, Signaling, Routing and MAC protocols for MANETs. In: Proc. of Telecommunication Networks and Applications Conference, 2008, pp. 97-102.

[14]. Rodrigo do Carmo, Marc Werner, and Matthias Hollick. "Signs of a Bad Neighborhood: A Lightweight Metric for Anomaly Detection in Mobile Ad Hoc Networks" in Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus. Copyright 2012 ACM 978-1-4503-1619-4/12/10