iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** II **Month of publication:** February 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Analysis of Trust Dynamics in Cyclic Mobile Ad Hoc Networks

Surbhi Hooda [1], Mrs. Rachna [2]
[1]M.Tech Scholar, [2]Assistant Professor
Department of CSE, Gateway Institute of Engineering & Technology, DCRUST, India

Abstract*—Mobile Adhoc networks are gaining popularity in today's dynamic environment. These are characterized by high mobility, infrastructure less, self-organizing, quick deployability and resource constrained networks. The network depends on cooperation among nodes for any communication. High mobility and dynamic architecture of mobile adhoc network make it vulnerable to security issues. Trust plays an important role for reliable and secured routing. To deal with the security issues in MANETS various trust models, reputation models and improved routing protocols are there but very less focus is given to the mobility pattern and dynamics of trust. In this paper, we modified the existing AODV routing protocol incorporating the trust dynamics and load balancing to deal with congestion and ensure secure routing in cyclic mobile Adhoc network. Fair Initialization and management of trust values is also considered during designing of this paper. The simulation is done using simulator NS2. Proposed work shows improvement over standard AODV protocol in terms of various network performance parameters.

Keywords*—congestion; mobile adhoc network; performance parameters; routing protocols; Trust; trust dynamics

I. INTRODUCTION

MANETS refer to mobile adhoc network with nodes possessing periodic motion. In Cyclic Manets the nodes appear repeatedly in the network and we have represented using circular motion but it can follow an irregular pattern also. Most of the trust approaches consider the fixed position models and less importance is given to the mobility. CTrust [1] scheme focuses on the mobility issue in detail considering the cyclic movement. Due to high mobility and frequent disconnections mobile adhoc network are vulnerable to security threats. Security issues are of prime importance which needs to be dealt with and various trust models are given for the same.

A lot of research has been done to ensure secure routing by various Trust models, Reputation system and new protocols. Trust based security enhances the performance of network and trustworthy behavior of mobile nodes. Various AODV modifications are given earlier but either they are complex in architecture, use cryptographic operations which are expensive and incur overheads or based on third parties for trust value. There is a need to develop protocols which are simple, less overheads and robust. Our work shows improvement over normal AODV in terms of network parameters like packet delivery ratio, throughput, message overhead and packet loss. It is simple in architecture, less expensive and incurs less overhead. Our contribution in the paper can be summarized as follows:

A. We simulate repeatedly moving mobile adhoc network in circular motion on network simulator NS2.

B. We analyze trust dynamics by modifying normal AODV protocol and secondly we also added load balancing strategy to deal with congestion that further improves our proposed work.

C. We draw comparison among normal AODV and our proposed routing protocols using graphs in terms of packet delivery ratio, message overhead, and throughput and packet loss.

The rest of the paper is organized as follows: Section II presents the Background. Section III presents the related works. Section IV presents proposed work. Section V presents simulation results and analysis and lastly Section VI gives the conclusion and future work.

II. BACKGROUND

A. Trust and Trust Dynamics

Concept of trust is multidisciplinary [2], different domains have different views about the idea of trust. Trust can be referred to as a belief in the qualities of other party or person that it will behave as expected when the opportunity occurs. Based on different domains the properties of trust and ways of computing trust vary. Trust can be direct or indirect based on the way it is computed. Direct trust is based on experience and observation where as indirect trust is based on the recommendation given by any third party.

Another is hybrid trust which is combination of both direct and indirect trust.

The trust on any node depends on the behavior of the node in the network, node can be highly trusted in one context but not in other. Properties of trust are dynamic nature, context dependency, subjective, asymmetric and composite [4]. Trust can be classified as risk, belief, subjective probability and transitive.

Trust Dynamics can be explained as the phases through which the trust passes or simply we can say the evolution of trust. Trust never remains constant; it changes with time, location, experience etc. Trust Dynamics [3] includes Trust Computation, Trust Propagation, Trust Aggregation and Trust Prediction. These are new areas of research in distributed adhoc networks.

1) *Trust propagation:* Trust Propagation is useful in sharing the trust values among the nodes in the network thus reducing overheads.
2) *Trust aggregation:* Trust Aggregation is used to estimate the final value of trust. As trust values are propagated in the network, thus for single node there are different values of trust from different nodes. Then to get the final trust value aggregation is done. The complexity of aggregation operations should be low.
3) *Trust Prediction:* Trust Prediction is used to predict the values of trust on the basis of present and past behaviors.

B. AODV Routing protocol

Ad-hoc On demand Distance Vector (AODV) routing protocol is a reactive protocol or on-demand protocol [16] that establishes the route only on demand and always search for the shortest path irrespective of reliability of the path. It does not have information about other nodes until any communication is needed. AODV also makes use of sequence numbers which ensure that routes do not have loops and determines the freshness of any route. The advantages include on-demand creation of routes, less connection set up delay whereas disadvantages are high bandwidth consumption, overheads in control messages. The major operations are Route Discovery and Route Maintenance and explained below:

1) *Route Discovery:* When source node wants to establish a connection, source node looks for the route to destination in its routing table. When there is no route available it sends RREQ packet to its neighbors. RREQ packet if forwarded until the destination is reached or the path to destination is found. The destination node sends the route reply message RREP, it travels the reverse route. Based on the minimum hop count the path is selected and it checks the destination sequence number which should be greater than destination sequence number of RREQ packet.
2) *Route Maintenance:* If there is any problem on the route, Route Error message (RERR) is sent to the transmitting node to inform about it and start the process of transmission again. HELLO messages are used by AODV periodically for Route maintenance.

III. RELATED WORKS

There have been works earlier in improving the security of mobile adhoc networks by improving routing protocols based on trust. Several survey papers summarize the concept of trust, properties of trust and different trust schemes. In this section we summarize some of the works done earlier:

Zhao *et al*. [1] gave the cTrust scheme based on cyclic mobile adhoc network, cMANET. CMANET are networks with cyclic movement pattern of nodes, presented the trust transfer function to transfer the trust values in case of indirect trust, trust value iteration function and proposed cTrust distribution trust aggregation algorithm.

Cho *et al*. [2] surveyed different schemes, attacks, performance metrics and trust metrics. It discusses about future research areas on trust management in MANETs based on the concept of social and cognitive networks. It discusses the concepts and properties of trust and derives some unique characteristics of trust in MANETs, drawing upon social notions of trust.

England *et al*. [3] provided overview of trust and trust management. They outlined the behavioral properties of nodes that are useful in calculation of trust. A summary of trust metrics used to record levels of trust, trust dynamics and how trust can change with time, experience and state with an outline into trust propagation, trust aggregation and trust prediction.

Govindan *et al*. [4] explain about the concept of Trust, properties of trust. It also surveys different approaches to computations of trust and gave the Manets trust system.

Pushpa [5], proposed trust based AODV protocol. Route Table and Neighbor Table are maintained at every node. Route Table has an entry as route trust field which stores detail of routes. Neighbor Table has two fields' neighbor_id and trust value which stores details of node trust.

Narayan *et al*. [6] propose congestion-aware multipath routing protocol. Network congestion is the main reason for lower throughput and longer delay. The protocol calculates the occurrence of congestion by monitoring and reporting average queue

utilization thresholds of multiple interfaces as QoS parameter and uses multiple paths to balance the load during the periods of congestion to improve quality of service.

Subramanian *et al*. [7] proposed trust based scheme which can be used to track untrustworthy nodes and isolate them from routing, thus provide trustworthiness. In this paper a trusted AODV (ST-AODV) protocol is presented which assigns a trust value for each node. A threshold value is assigned and if the nodes trust value is greater than this value its marked as trustworthy node and allowed to participate in routing else the node is marked untrustworthy.

Xiaoqi Li *et al* [8] have proposed a model based on Trust and modified AODV. Routing table has three additional fields' positive events, negative events and opinion. Based on positive and negative evidences about other node, opinion about that node is determined. Discounting Combination and Consensus Combination operations are used to get the overall opinion. It detects and eliminates malicious nodes as time passes.

Khurana *et al*. [9] proposed the extended AODV called RAODV by adding two new control messages. RRDU messages are sent by source node to the destination at regular intervals along with the RRDUID. RRDU_REP is the response message which is sent by destination to source node. The routing table is modified using Reliability List field. RL field consists of source address, forward data packet (FDPC) and RRDU-ID. HELLO messages for route maintenance.

Mangrulkar *et al.* [10] proposed TBAODV to improve the route selection mechanism using trust parameter. This trust parameter is introduced in the route request format which is updated on every successful data transmission.

Sridhar Subramanian *et al.* [11] proposed trust based reliable AODV abbreviated as TBRAODV. It is able to detect the misbehaving nodes and mark them untrustworthy. Based on the trust value the behavior of node is determined as trustworthy or not. Only reliable nodes are allowed to participate in routing for reliable routing of data and unreliable nodes are not allowed to participate. The advantage of this approach is it identifies the bad nodes already.

Sharma *et al***.** [12] proposed trust based secure AODV protocol. It also uses two new routing messages. Trust update policies are used to update trust depending on occurrence of positive event, negative event and thus change in the opinion will be calculated. It uses the concept of Requestor, Recommender and Recommendee based on who is issuing TREQ, TREP and TWARN (trust warning message) messages.

Islam *et al.* [13] proposed explicit no technique in which EXPLICIT NO packet is used. Any node when not available in the network informs the source node by sending EXPLICIT NO packet. It has simple architecture and energy conserving. It has limitations in terms of overheads and non availability of nodes as it sends EXPLICIT NO packet to inform the source node even it has high trust value.

Wadbude *et al*. [14] proposed an efficient secure AODV routing protocol, using Hash chains, Digital Signature and Protocol Enforcement Mechanism to secure packets in AODV. Hash Chain is used to secure the Hop count. SAODV includes another feature which allows intermediate nodes to reply to RREQ message.

For a single message the signature needs to be generated and verified when it receives RREQ and similar for RREP. Intermediate nodes can store this second signature in their routing table along with other routing information. If one of the nodes receives a RREQ message it can reply with RREP message similar to AODV. To achieve that intermediate node generates the RREP message which includes the signature of source node and signs the message with its own private key. This is called double signature.

Simaremare *et al.* [15] proposed AODV routing protocol based on trust mechanism using the concept of local trust and global trust. Local trust is in reference to specific nodes based on received packet and forwarded packet whereas global trust is total packet received and total packet forwarded in the network. Trust calculation is done before communication starts. It is able to handle Blackhole attack and Dos attack in the network. The limitation is that nodes work in promiscuous mode which is not active in AODV.

IV. PROPOSED WORK

We have modified AODV routing protocol based on trust. Trust dynamics refers to evolution of trust with time. The normal AODV protocol finds shortest route in the network for transmission of data. It does not check for the reliability of path. In our proposed work, initially we have added the concept of trust and its dynamics analyzed it using simulator. Secondly, to deal with congestion issues in the network we also added the load balancing strategy to our proposed approach. The results are analyzed using graphs comparing Normal AODV, our proposed trust AODV and trust and load balancing AODV. Results show that our trust based AODV is improved and when we further add loadbalancing there is more improvement shown in packet delivery ratio, reduction in message overhead, high throughput.

A. Architecture

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The conceptual architecture of the proposed work is given in Fig.1 below and the detailed explanation is discussed in implementation subsection.

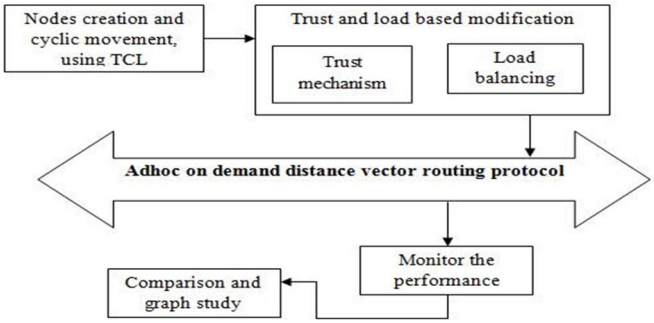


Figure.1 Proposed Work Architecture

B. Algorithm

1) Trust initialization

a) Assign node ID (node_id) to the new node by MANET protocol.

b) The new node's initial local trust table is established by direct transactions.

c) The new node is always given a default trust value 0.5

d) Initially a node is aware of trust values of its just neighbors.

2) Trust Calculation and Aggregation

a) Initialize local trust for nodes.

b) for each node *i* in cMANET if node *i* want to communicate with node *j*

c) We aggregate the values of trust to find path trust, T_p using summation operator.

d) For each path for which the T_p is calculated as a route response, we select the path with greatest T_p

e) Follow the link path for data communication among the nodes.

3) Trust updations Algorithm

a) Default local trust value, T_D

b) Initialize packet drop, *d* to 0;

c) For each packet drop in the network we find total packets dropped {

D=d++

}

d) Decrement trust value if *D* is greater than critical trust value i.e.

if(D=>critical_trust_value) {

$T_D = T_D - 1$;

}

e) Otherwise increment the value of trust as reward of good behavior.

4) For a set of available paths from source to destination

a) For all paths available from source to destination
calculate the default path length (hop count) initially

b) Select max 10 paths from available list.

c) For all paths in available
Select a set of paths having minimum path length.
Choose available best path for Communication.

d) Update the path according to load during route update procedure of routing protocol (AODV)

e) Repeat the steps from 3 to 6 for each route update.

f) Exit()

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Implementation

1) *Cyclic Manet formation:* we design our scenario in NS-2, using tcl scripting. Initially there are 10 nodes in the network and maximum of 40 nodes. Motion of nodes is repeated in circle to simulate cyclic movement pattern.
2) *Trust initialization:* initial trust value assigned is 0.5 to show fair behavior. We create trust_store class which stores the values of trust. We create functions for trust entry and insert the trust value.
3) *Trust updations (deletion and aggregation):* trust values are updated according to the nodes behavior in terms of packet dropped. When node is not active for long trust delete function is called.
4) *Load balancing:* when there is congestion on the trusted path, load balancing strategy is activated. The other best available path is selected, which is trustworthy as well as balanced in node.
5) *Comparison and result:* The output results are logged in trace files. Results are either text-based or animation based. We use XGRAPH and network animator (NAM) tools to show results interactively. The comparison of the approaches are done using excel graphs.

V. SIMULATION AND RESULTS

A. Simulation environment

Our proposed approach is simulated using network simulator NS-2.35. NS-2 is discrete event simulator based on two languages: c++ and otcl(object oriented tool command language). C++ is backend language and otcl is used to create simulation by assembling and configuring objects as well as schedule events. To analyze particular results trace from overall results excel graphs are drawn for conceivable presentation. Simulation parameters table is shown below in table1:

TABLE1. SIMULATION PARAMETER TABLE

Parameter	Value
Simulator version	NS-2.35
Min no. of nodes	10
Max no. of nodes	40
Routing protocol	AODV
Traffic type	TCP
Simulation time	20sec
Packet size	512

The simulation scenario for 10 nodes is shown on NAM below in fig.2

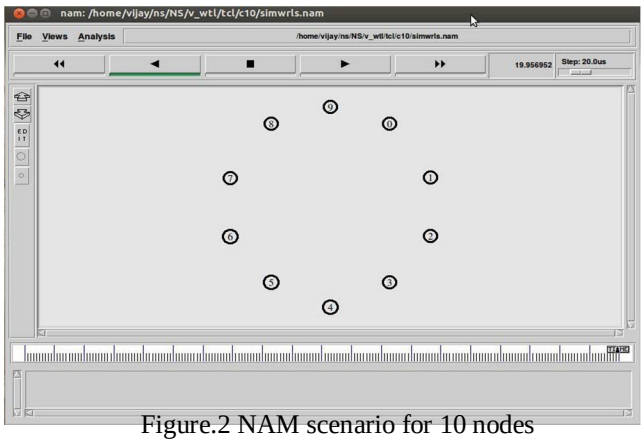


Figure.2 NAM scenario for 10 nodes

Volume 4 Issue II, February 2016
ISSN: 2321-9653

Xgraph for delay in 10 nodes network is shown separately for three cases below in fig.3, fig.4 and fig.5.

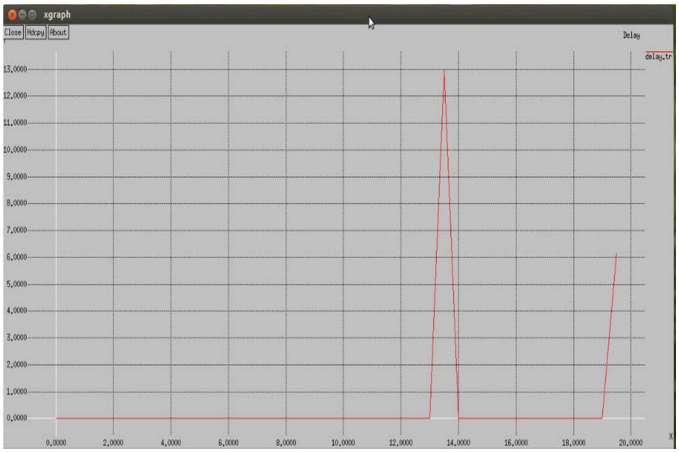


Figure.3 Delay in normal AODV

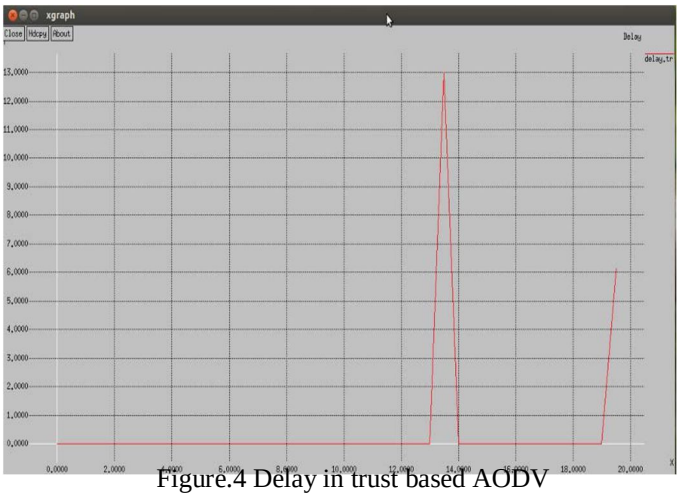


Figure.4 Delay in trust based AODV

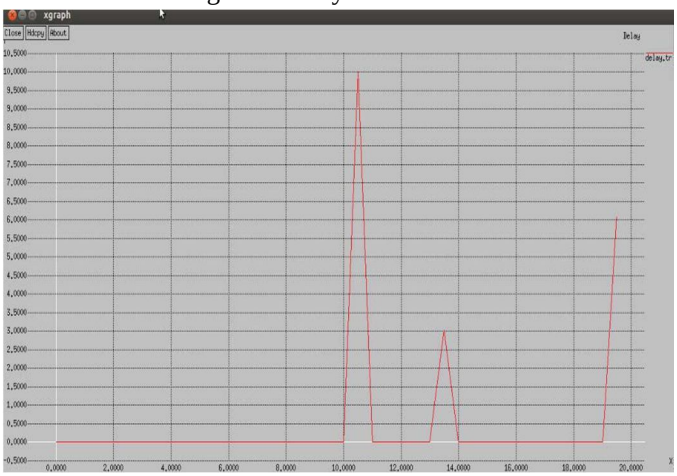


Figure.5 Delay in trust and load based AODV

B. Performance parameters

The performance parameters used for comparison of the Normal AODV, trust modified AODV and trust and load balancing based AODV are packet delivery ratio(PDR), message overhead, throughput and packet loss.

1) *Packet Delivery Ratio:* pdr is improved in our trust based AODV, and when load balancing is applied there is further increase. It is shown in fig.6 below

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

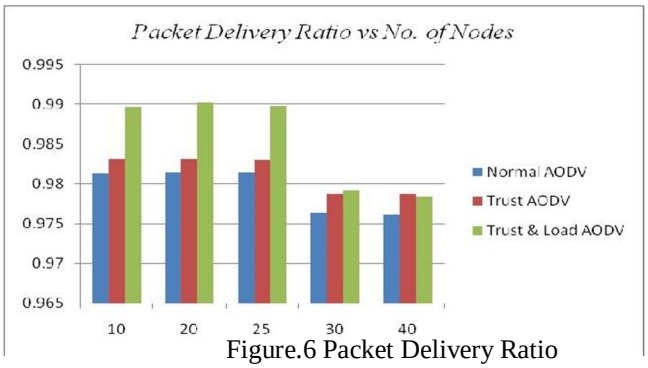


Figure.6 Packet Delivery Ratio

2) *Message Overhead:* overall overhead is reduced in trust based AODV, but is greatly reduced in our work when we apply trust and load balancing concept both together. It is shown in fig.7 below

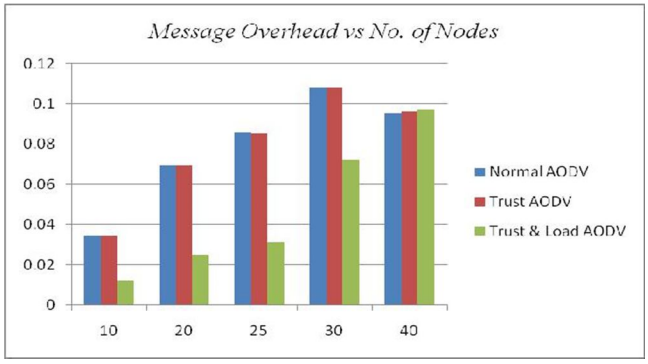


Figure.7 Message Overhead

3) *Throughput:* it is improved in our proposed work and shown in fig.8 below:

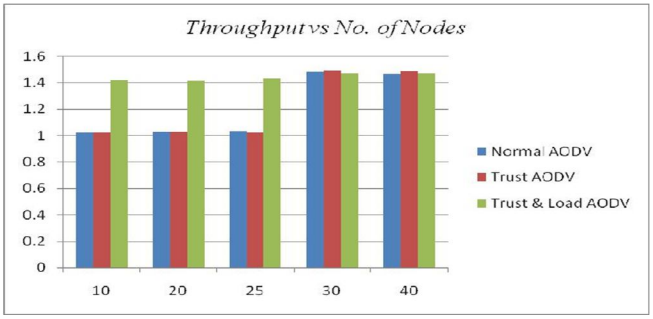


Figure.8 Throughput

4) *Packet Loss:* packet loss is less in our proposed work and is shown below in fig.9

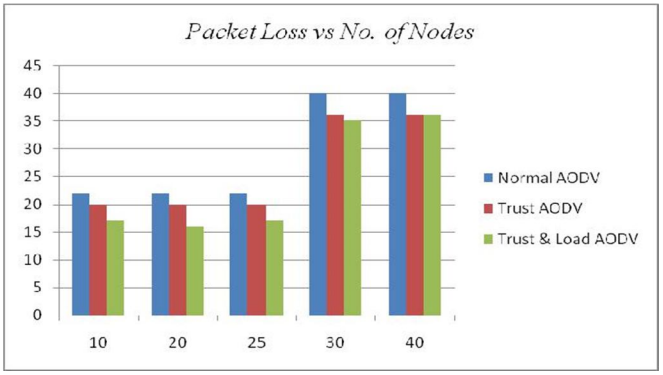


Figure.9 Packet Loss

VI. CONCLUSION & FUTURE WORK

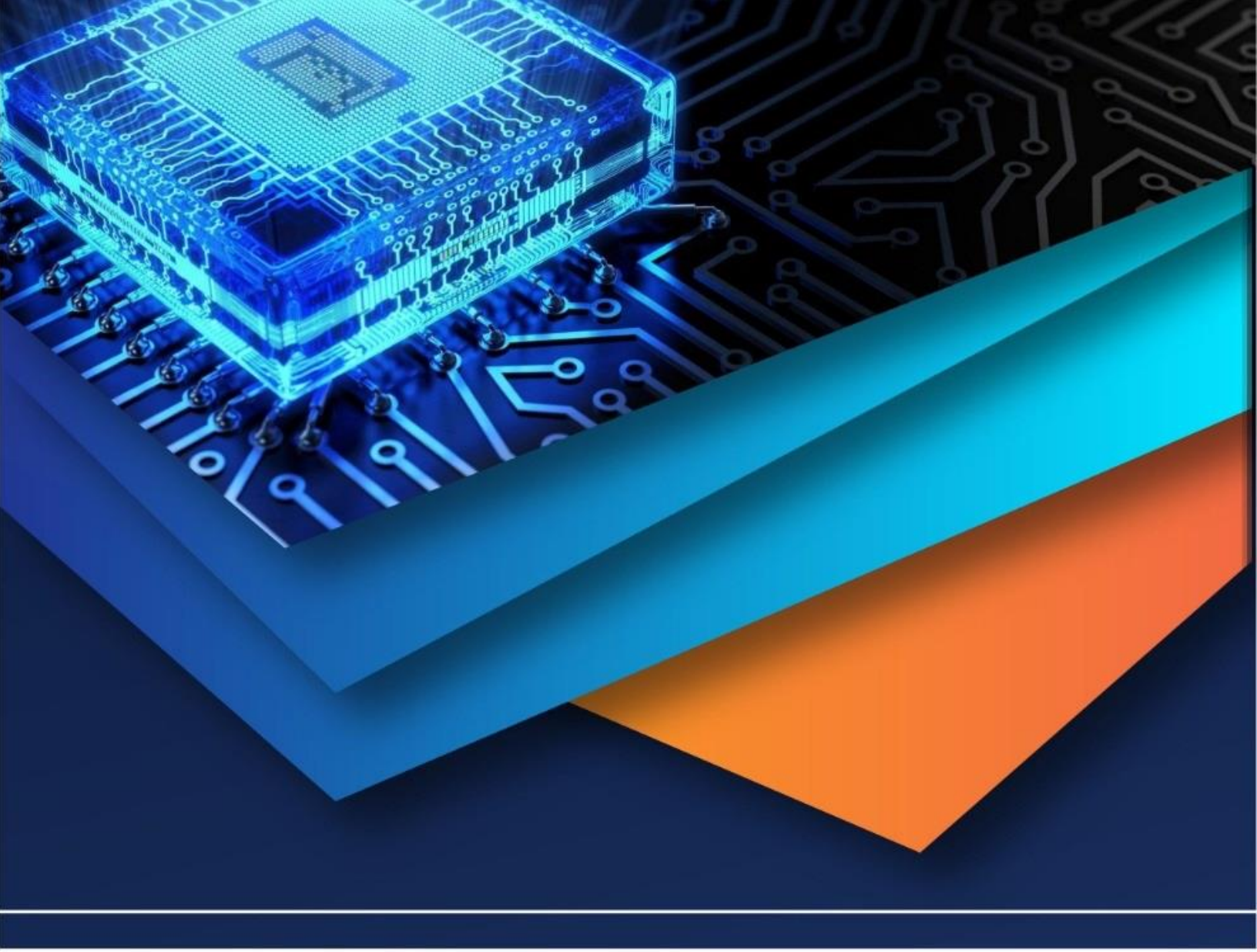
The simulation study of cMANET using trust and load balancing mechanism shows that use of trust model is an effective measure to counter the maliciously behaving nodes especially in cyclic MANETs. Load balancing measures gives alternative paths to be used when there is congestion like condition in the network during packet flow. The trust dynamics is analyzed on basis of AODV routing protocol using various network parameters. In future, the load balancing mechanism can be enhanced to be applied over a set of routing protocols and the impact of network dynamics on trust dynamics.

VII. ACKNOWLEDGMENT

This paper is made possible through the support and institutional facilities provided by the Department of Computer Science & Engineering, GIET sonipat. We convey our sincere thanks to other M.Tech scholars for their rigorous brainstorming sessions to shape up this research paper.

REFRENCES

[1] Huanyu Zhao, Xin Yang, and Xiaolin Li. ” cTrust: Trust Management in Cyclic Mobile Ad-hoc Networks”, in IEEE transactions on vehicular technology, vol.62, no.6, July 2013
[2] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, “A Survey on Trust Management for Mobile Ad-Hoc Networks”, in: IEEE communications surveys and tutorials, vol.13, no.4, pp. 562-583, fourth quarter 2011.
[3] Philip England, Dr Qi Shi, Dr Bob Askwith and Dr Faycal Bouhafs, “A Survey of Trust Management in Mobile Ad-Hoc Networks”, in Proceedings of the 13th annual post graduate symposium on the convergence of telecommunications, networking, and broadcasting, PGNET. 2012
[4] Kannan Govindan and Prasant Mohapatra,” Trust computations and Trust dynamics in Mobile Ad-hoc Networks: A Survey”, in: IEEE communication surveys and tutorials, vol. 14, no. 2, pp.279-298, second quarter 2012
[5] A.Menaka Pushpa, “Trust Based Secure Routing in AODV Routing Protocol”, in Internet Multimedia Services Architecture and Applications (IMSAA), IEEE conference, pp.1-6 , 2009.
[6] D.G.Narayan, R.Nivedita, S.Kiran and M.Uma, “ Congestion Adaptive Multipath Routing Protocol for Multi-Radio Wireless Mesh Networks”, in International Conference on Radar, Communication and Computing, pp.72-76, December 2012.
[7] Sridhar Subramanian and Baskaran Ramachandran, “QOS Assertion in MANET Routing Based on Trusted AODV (ST-AODV) “, in International Journal of Adhoc, Sensor & Ubiquitous Computing, vol.3, no.3, June 2012
[8] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, “A Trust Model Based Routing Protocol for Secure Ad Hoc Networks”, in Aerospace Conference, 2004. Proceedings, vol.2, pp. 1286-1295, 2004.
[9] Khurana Sandhya, Neelima Gupta and Nagender Aneja, “Reliable ad-hoc on-demand distance vector routing protocol”, in Networking, International Conference on Mobile Communications and Learning Technologies,2006. International Conference on IEEE, pp.98-98, 2006.
[10] Mangrulkar, R. S., Pallavi V. Chavan, and S. N. Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT." in International Journal of Computer Applications (0975–8887) Volume. 36-39, 2010
[11] Subramanian, Sridhar, and Baskaran Ramachandran. “Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks.” arXiv preprint arXiv:1202.1664,2012.
[12] Sharma, Pankaj. "Trust based secure aodv in manet. " Journal of Global Research in Computer Science, vol.3, no.6, pp.107-114, June 2012.
[13] Islam, M. Hassan, and Misbah Zareen. "Mitigating the effect of malicious node in Mobile Ad Hoc Networks using Trust based Explicit No Technique. "International Journal of Computer Networks and Communications Security, vol.1, no.6, pp.210-215, November 2013
[14] Wadbude, Durgesh, and Vineet Richariya.”An Efficient Secure AODV Routing Protocol in MANET.” International Journal of Engineering and Innovative Technology(IJEIT), vol.1, pp.274-279, April 2012.
[15] Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. “Secure AODV Routing Protocol Based on Trust Mechanism.” in Wireless Networks and Security, Springer Berlin Heidelberg, pp. 81-105, 2013.
[16] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY