Dispersed Opinion based QoS Cognizant Routing Protocol against Black hole Attack in MANET

Vijay Kumar Singh[1], Piyush Kumar Shukla[2], Sachin Goyal[3]

[1](Department of Computer Science and Engineering, Bansal College of Engineering, Mandideep, Bhopal, Madhya Pradesh, India,

[2](Department of Computer Science and Engineering, University Institute of Technology, Bhopal, Madhya Pradesh, India)

[3](Department of Information Technology, University Institute of Technology, Bhopal, Madhya Pradesh, India)

Abstract: *MANET is an infrastructure fewer network, here each node acts as à router and so capable to forwards data packets to all other neighboring nodes. Hence, the routing packet overhead has been reduced. Routing in MANETs is challenging since the network topology is dynamic, self- organized, self-administrated and low transmission range. Due to the above characteristics, MANET is vulnerable to various attacks like routing attacks, DoS (Denial of Service) MANET is an infrastructure fewer network, autonomous system, which is a collection of mobile nodes. This paper is based on analysis of trust based source routing using the trust prediction system in mobile ad-hoc network. Here, a trust based source routing protocol using QoS constraints has been designed. In this paper, the Trust prediction system has been designed for checking the trustworthiness of the nodes present in the network. Trust prediction finds the best route for the source based routing that is free from malicious nodes effect. In this paper DTQR (Dispersed Trust based QoS aware routing) has been designed & implemented for preventing the malicious nodes from entering the network. We also compare the DTQR (Dispersed Trust based QoS aware Routing) algorithm with TQR (Trust based QoS aware Routing) and Watchdog-DSR. The Simulation results show that the DTQR prevents an attack from malicious nodes and the security, performance, the packet delivery ratio, detection ratio of malicious nodes, data receiving analysis, has been improved.*

Keywords: *Trust Prediction, Trust Analysis, degree, Watchdog DSR, Malicious Node, QoS Constraints*

I. Introduction

Mobile Ad hoc Network (MANET) [3] is a set of mobile nodes, with no centralized administration or no fixed infrastructure. MANET is a stand-alone and autonomous communication network. [16] The infrastructure of MANET is unpredictable and due to dynamically change in topology, the routing of data is promising.

Ad-hoc networks have various applications such as in healthcare application, military applications. Battlefield applications where wired connections of fixed infrastructure is impossible or maintained. For example, Wireless fidelity, i.e. Wi-Fi (IEEE 802.11) protocol is capable of ad-hoc networking, where the access point is unavailable. In IEEE 802.11, it restricts the node to receive or send the data packets that do not participate in the network or routing. MANET (Mobile ad hoc network) is an infrastructure-less network, which consists of various numbers of mobile nodes. The network in MANET is dynamically established without any centralized administration. In MANET [21], mobile nodes make certain tasks that are challenging since they have limited resources like memory, storage, CPU.

In **Fig. 1,** we consider a network with four mobile nodes. Where node A is the source and node D is a destination node. B and C are intermediate nodes through which A can communicate with node D. Hence the route for transmitting data packets is A-B-C-D.

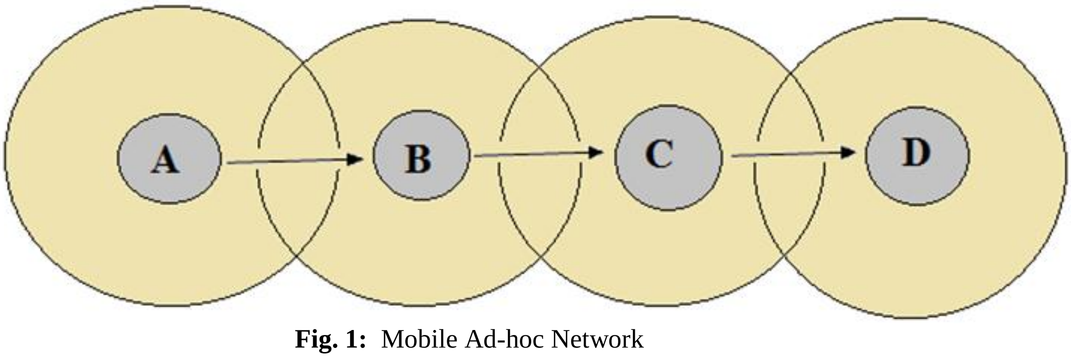

Fig. 1: Mobile Ad-hoc Network

Various Trusts used in the Models

Every node contains a pair of public and private keys in Public Key Infrastructure. Public keys are common that is dispersed to all nodes evenly. But private key is known only to the node, no other node can access that key that is required for providing security to the system. In Digital Signatures, the Certificate Authority (CA) is used for distributing the public keys and private keys to the sender and receiver for checking the authentication of certificates.

MOCA [23] (Mobile Certificate Authorities) is a technique in which CA (Certificate Authority) is Dispersed over some nodes that are specially chosen through their physical features and their security. In the MOCA protocol, node requires a certificate and sends requests for certification, i.e. CRQ (Certification Request) packets to MOCA, and then MOCA responds to CRQ packet with CREP (Certification Reply) which consist of a fractional signature. The node constructs a complete signature using a number of CREP packets. CREQ packets are same as RREQ packets and CREP packets are same as RREP packets. The drawback of MOCA is the overhead of number of fractional signature and the delay for generating a complete signature.

A trust model is implemented for MANET, in which each and every node signs in certificates of other nodes [25]. Transitive trust is required in this trust model. If P trusts Q, and Q trusts S, then P will also trust S. The chain of certificates is followed in which nodes authenticate the message. When various nodes lie between the sender and receiver, an attacker must have to compromise a node in each and every path so that the network gets compromised. But, the network limits the certificate's length for the nodes such that an attacker cannot enter the network easily.

Certificate authority [24] invalidates the certificate for public key of a node when a node gets compromised. Hence a mechanism is required that can prevent attacker from invalidating the keys. But this problem is more complicated than the key management problem. A mechanism can be followed where the block list of nodes and information related to the invalidation of certificates of nodes can be broadcasted to nodes in the network when invalidation of certificates occurs. But, the broadcasting is limited such that no attacker other than nodes of the network may receive this information.

Intrusion is defined as a set of events to alter or compromise the availability, integrity, confidentiality of resources or unauthorized activities in a network. An IDS [25] is a system that detects and gives alert on various misbehaviors in a network or system. The proactive routing solutions alone are not enough to prevent from the intrusion, attacks. Hence IDS [25] was implemented.

In Fig 2 Direct Trust has been explained, **Fig 2** shows that node C wants the trust degree of node B, but link directly from node C to node B is unavailable. Node C indirectly inherits the trust of node B through node A. This trust is known as indirect trust.

Fig 3 shows that Node A wants the trust degree of node B, but a link is available from node A to node B. this is known as direct trust.

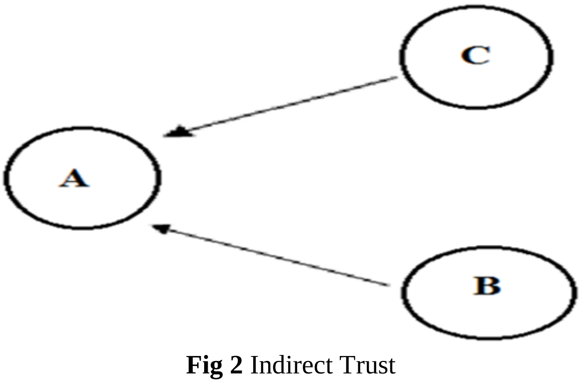

Fig 2 Indirect Trust

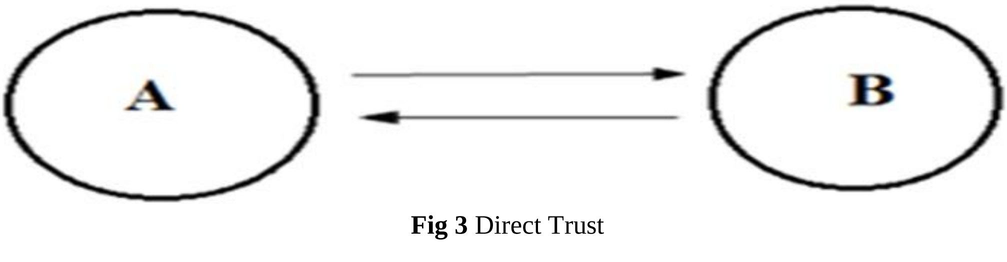

Fig 3 Direct Trust

II. Proposed Work

Mobile ad-hoc network is a temporary autonomous network system, where every communication takes place in trust basis, but does not guarantees that our data will be successfully delivered to a legitimate user. Before this proposal we studied number of papers related to quality of service, trust mechanism, reliability and security against different attacks in MANET, but they does not cover all aspects of network parameters and also identifies that some improvement is needed in the existing work. Therefore, in the proposed approach we design a Dispersed trust methodology that achieves the QoS requirement for reliable service. In Dispersed trust mechanism every node watch the activity of neighbor nodes and calculate the trust level based on data received and forwarding criteria, whereas the trust level ranges between 0 to 1. The trust factor by every neighbor nodes are calculated by timely manner, and combine the trust level of particular node (suspicious) in the single area (whose reliability or trust level all the node set initially 1), that node calculates average trust value of particular node (suspicious) and while trust values lower than the fifty percentage so further that is under second time (suspicious) re-watch the node and similar property exist than block that particular node else trust level increases. That work collaboratively calculates the node trust and time to time increase trust level of the node and helps to identify attacker node. In our approach trust level calculated against the black hole attack, here trust level cannot decrease until data has drop by network depended reasons i.e. congestion, collision, MAC error etc. Proposed approach provides the reliable path from sender to receiver with all aspect of QoS requirements. That increases the packet delivery ratio, packet received & attack detection ratio of the network.

In **Fig. 4**, trust management consists of four elements i.e. trust calculation, trust estimation, trust establishment, and trust updation.

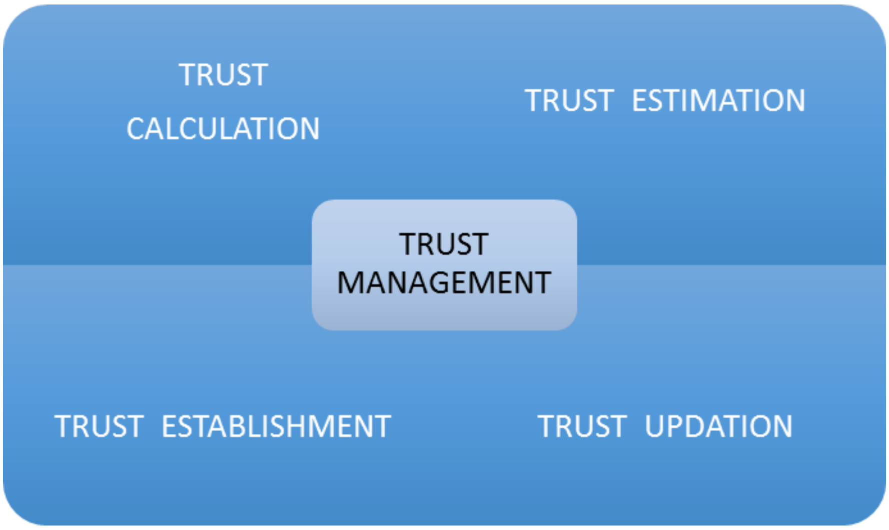

Fig. 4 Trust Management

ATION

III. Proposed Algorithm

# CALCULATE **DTQR**

Input:

M_n: Set of Mobile Nodes

S_n: Suspicious Nodes

n_n: Set of Neighbor Nodes

D: Set as trust calculator node

$T_{x:}$ Transmitter node

$R_{x:}$ Receiver node

In: Set of intermediate nodes

msend: Mis Detected

tsend: Trusted Send

P_{tf} :Number of Packets Forwarded.

$Pt_{r:}$ Number of Packets Received

$T_{dc}r$= Decreased Trust

$T_{nl:}$= New Trust Level

Time Start=T_{start}

Time End=T_{end}

Output:

Attacker node information, PDR, Receives and Sends Information

```
T ← execute-route ($T_x$, $R_x$, DTQR)
# DTQR algorithm
Begin
Initiate $T_x$ ← execute-route($T_x$, $R_x$, DTQR)
While ($M_n$ =in range)
do
{
    $I_n$ ← receives routing packets
    For each $I_n$ in range , $n_n$ watch the $I_x$ and set $S_n$
    While $S_n \neq R_x$
    do
    {
    Calculate Trust of $S_n$: ($P_{tf}/Pt_r$)
        If ($R_x = S_n$ ) then
        {
            Send Ack to $_{Tx}$ node
            Call data-pkt()
        Else
            $R_x$ not in zone
        }
    }
}
Data-pkt($T_x$ ,$R_x$, pkt)
{
    Count =1
    If path is available then
    {
        All node in path set $S_n$
        $n_g$ watch $S_n$ node
    }
}
While Packet incoming $S_n$
do
{
    If $S_n$ receives && pkt-forward $\neq$ true then
    {
        $T_{dc}r = S_{old\text{-}trust} - P_{tf}/Pt_r$
        $S_n$ ← $T_{nl}$
    Else
    {
        Increase-trust = S-old-trust + ($P_{tf}/Pt_r$)
        $S_n$ ← new-trust-level
    }
    }
    all $n_n$ calculate separately trust level of $S_n$ node
    $n_n$ send trust report to D node
    D calculate average trust level of $n_g$ for S node
}
While count <= 2
do
{
    Re-calculate the trust of S
    Increment count
}
If count == 2 && trust level of $S_n$ < 0.5 then
{
    Block the $S_n$ and set attacker
Else
Enter $S_n$ in trusted group
}
Calculate PDR = $(P_{tr}/P_{tf})*100$
Packet Duration = $T_{end}$ - $T_{start}$;
if packet_duration > 0  then
 sum += packet_duration;
 recvnum++;
  Attack% = [100-(msends/tsend)*100];
}
End
```

IV. Simulation Parameters

In this work, the performance analysis is done in MANET (Mobile ad-hoc Network) that is based on IEEE 802.11b MAC layer. The simulation is done under saturated Condition. The Simulation is performed using NS-2.31. The number of nodes present in the network is defined previously i.e. 50 nodes. When simulation is performed in the simulation area of 800 m *800 m, the mobile nodes move randomly in any direction. The routing protocol used is DTQR that is based on AODV protocol. The routing is performed in presence of malicious nodes under the black hole attack. The UDP/CBR [5] is used as transport protocol/ traffic source. The simulation is performed till 900s. 7 simulations each of 150 s are run during each performance factor. In simulation, the following time has been taken 0 s, 150 s, 300 s, 450 s, 600 s, 750 s, 900 s. The packet size is 512 bytes and uses random way mobility model. The five performance plots is compared i.e. Simulation time vs. packet delivery ratio, Simulation time vs. receiving packets at destination nodes, Simulation time vs. end-to-end delay, Simulation time vs. detection ratio of malicious nodes, Simulation time vs. routing packet overhead.

The trust value update improves the performance of the network and trustworthiness of nodes. The trust table is maintained for every node; hence no malicious nodes enter the network. Each simulation is repeated 50 times and average results are calculated.

Table 1: Table of Simulation Parameters, It shows the simulation parameters that have been used in the mobile ad-hoc network for performing the simulation. In the following parameters, the performance is analyzed in the network.

Parameters	Values
Simulation area	800 m *800 m
Simulation Time	900 s
Number of nodes	50
Number of malicious nodes	2
Connection Type	CBR/UDP
Packet Size	512 Bytes
Transmission Radius	250 m
Mobile Speed	20 m/s
Trust threshold degree	0.5
Trust time update	1 s
Physical, MAC layer	IEEE 802.11b
Mobility	Random Waypoint Model

V. Results & Analysis

5.1 Detailed Results: In this proposed work, we compare the DTQR with other protocols: TQR and Watchdog-DSR. TQR is a routing protocol that uses AODV protocol with trust and QoS constraints that improves packet delivery ratio, end-to-end delay. Watchdog DSR uses DSR routing protocol and Watchdog mechanism is used for detecting the malicious nodes in the network.

5.1.1 Packet Delivery Ratio: The ratio of total number of packets received by a node to the total number of packets sent from source. The Packet delivery ratio in routing protocols increases slowly as the simulation time increases since in trust–based model, source nodes only selects trusted and nodes present in optimal route and the Packet delivery ratio is enhanced. The packet delivery ratio is seen well in DTQR than in Watchdog-DSR and TQR. The PDR is better as Watchdog-DSR and DTQR is based on AODV protocol. And TQR is based on trust calculation implemented on it.

$$\text{Packet Delivery Ratio (PDR)} = \frac{\text{Number of Data packets Received by a destination node(D)}}{\text{Number of Data packets sent by a source node(S)}} * \mathbf{100}$$

Time (in secs)	**Packet Delivery Ratio**		
	DTQR	**TQR**	**Watch Dog- DSR**
0	0	0	0
150	46.02	41.02	37.07
300	59.87	55.59	51.30
450	76.97	68.51	60.86
600	84.05	70.67	66.32
750	89.92	87.23	74.35
900	97.88	93.50	73.39

5.1.2 Receiving Packets at Destination nodes: The ratio of total packets sent from a source node to destination to the total packets received by the destination node. Source nodes send data packets to the destination nodes through routing protocols. In the above table, we compare the Data packets received through the routing protocols DTQR, TQR, Watch Dog-DSR. We can see that the maximum data packets can be received through our proposed algorithm, DTQR.

The sending packets to these protocols are as follows:

Time (in secs)	**Sent Data Packets**
0	0
150	7498.00
300	15111.02
450	22730.01
600	30349.02
750	37969.04
900	45589.02

Time(in secs)	**Received Packets by Nodes**		
	DTQR	**TQR**	**Watch Dog- DSR**
0	0	0	0
150	3376.00	2998.00	2699.00
300	8889.00	8248.00	7588.00
450	17248.00	15098.00	13579.00
600	25194.00	21112.00	19792.00
750	33689.00	32724.00	27809.00
900	44123.00	42123.00	32949.00

5.1.3 Detection Ratio of Malicious Nodes: Detection Ratio is defined as the ratio of number of the detected malicious nodes to the total number of malicious nodes present in the network or topology. As Watchdog-DSR and TQR is also good in mitigating the malicious nodes. The detection ratio of DTQR is good than TQR and Watchdog-DSR. The detection ratio of routing protocols increases as the simulation speed increases. DTQR is capable of mitigating the malicious nodes more accurately.

Detection Ratio of Malicious Nodes: the ratio of number of malicious nodes detected to the actual number of malicious nodes is termed as detection ratio.

$$\textbf{Detection ratio of malicious nodes} = \frac{\textbf{Number ofDetected malicious nodes}}{\textbf{Total Number of Malicious nodes in the network}}$$

Time (in secs)	**Detection Ratio of Malicious Nodes**		
	DTQR	**TQR**	**Watch Dog- DSR**
0	0	0	0
150	64.60	57.66	53.00
300	78.96	73.47	68.77
450	83.00	79.82	74.53
600	89.82	86.43	76.09
750	94.69	91.93	85.33
900	102.00	96.34	85.34

5.2 Analysis of Results:

Fig 5 shows variation in Packet Delivery Ratio. DTQR is compared with Watchdog-DSR and TQR and results show that DTQR shows better results than Watchdog-DSR and TQR.

Fig 6 shows variation in data receiving packets. DTQR shows better performance than Watchdog-DSR and TQR.

Fig 7 shows detection ratio of malicious nodes through these protocols. DTQR shows better performance than Watchdog-DSR and TQR protocols.

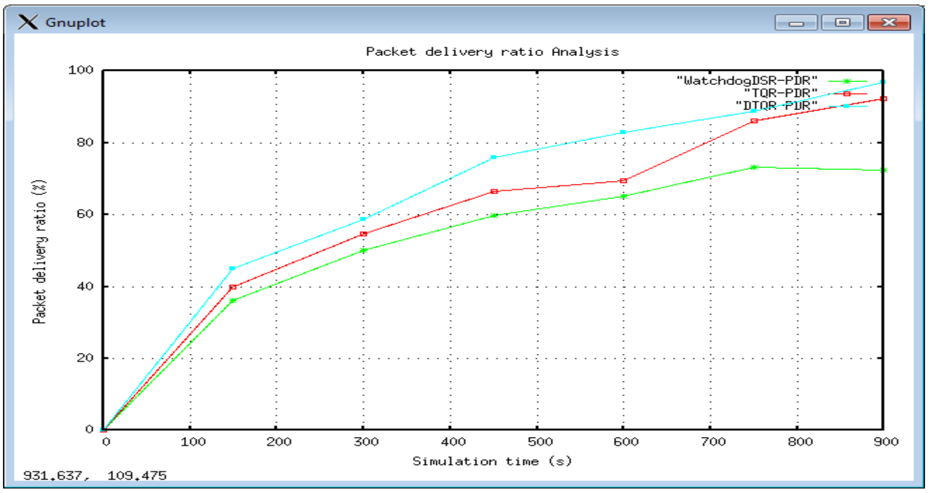

Fig 5: Variation of Packet delivery Ratio

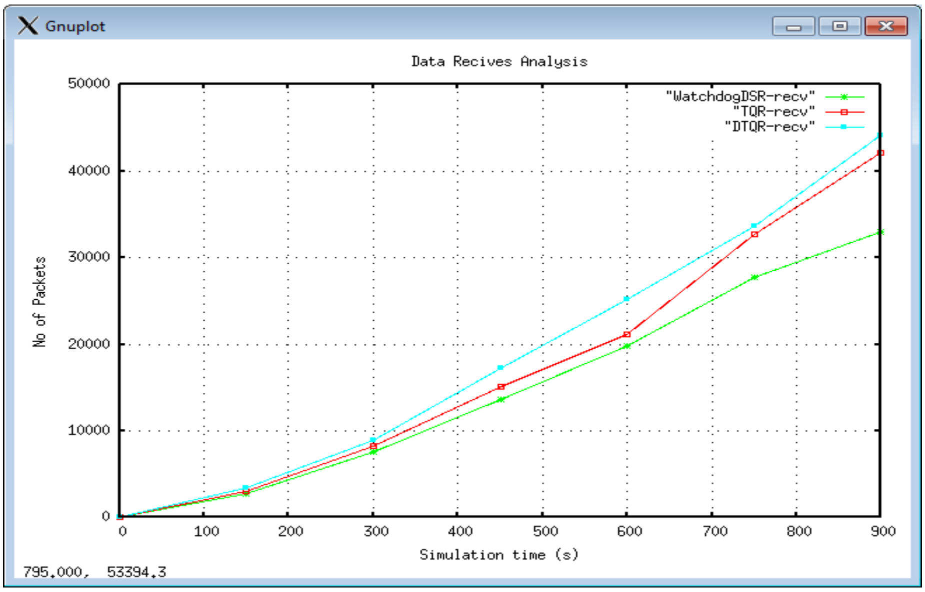

Fig 6: Variation of Data receiving analysis

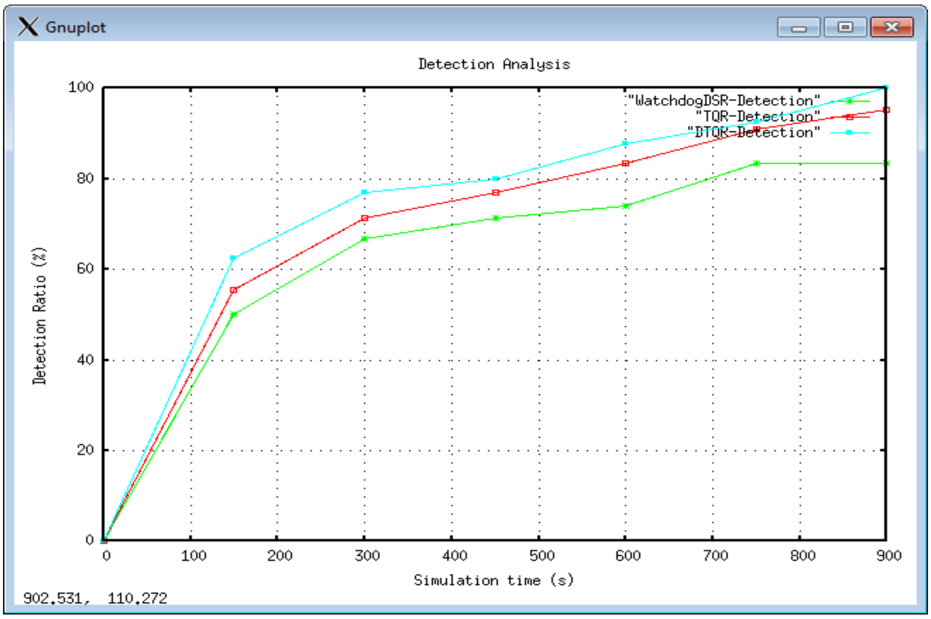

Fig 7 Variation of Detection Ratio of malicious nodes

The simulation is done under saturated Condition. The saturation condition determines that the sender node S always has a data packet to send to its intermediate nodes, and the buffer is non-empty. The mobile nodes are dispersed randomly in the network. The simulation used in the network simulator is random way mobility model. The random way mobility model is used commonly in experiments and simulations. Before simulation is performed the node chooses the area for simulation and chooses x and y coordinates. Once all the nodes are set in the network, the simulation is performed. When the simulation starts, it simulates for various time duration till 900s. The performance of DTQR protocol is performed in the basis of packet delivery ratio, receiving data packets analysis, end-to-end delay analysis and detection ratio of malicious nodes and routing packet analysis with respect to the simulation time. Our approach improves the throughput by. It is analyzed and computed that as the packet delivery ratio increases, the throughput also increases. And hence DTQR is better and provides better packet delivery ratio than TQR and Watchdog-DSR.

VI. Conclusions

In the proposed work, a trust mechanism based on Ad-Hoc on Demand Routing protocol termed as DTQR (Dispersed QoS aware Trust based routing protocol) is implemented. The proposed work uses Watchdog mechanism that is a higher implementation of Intrusion Detection System (IDS). DTQR detects the malicious nodes present in the network and improves the packet delivery ratio and packet receiving ratio and computes the trustworthiness of the nodes at various parameters. The DTQR protocol is implemented using NS-2 simulator based on AODV protocol and is compared with Watchdog-DSR and TQR in the presence of malicious nodes in the network. DTQR shows beat performance for the above parameters in the simulation. Through DTQR protocol, we can choose a best trusted path with trusted nodes and QoS constraints.

Dispersed Trust Based QoS aware routing protocol (DTQR) is compared with the Watchdog- DSR and TQR protocol on the basis of detection ratio, packet delivery ratio, packet receiving ratio while increasing the mobility of the network as well as increasing the malicious nodes in the network. It is observed that the proposed protocol performs better then Watchdog- DSR and TQR.

In our future work, we can compare the DTQR protocol with existing protocols and improve the performance using key management techniques and secure routing.

References

[1]. B Wang, X Chen, W Chang, A Light- Weight Trust-Based QoS Routing Algorithm for Ad Hoc Networks, International Journal of Pervasive and Mobile Computing, Elsevier, 13 (2), 2014, 164-180.

[2]. Chintan Kanani, A. Sinhal, Ant Colony Optimization based modified AOMDV for multipath routing in MANET, International Journal of Computer Application, 82 (10), 2013, 14-19.

[3]. R.K. Bara, J.K. Mandala and M.M Singh, QoS of MANET through trust based AODV routing protocol by exclusive of Black hole attack, First International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), Procardia Technology, Elsevier, Nirjuli, Arunachal Pradesh, India, 2013, 530-537.

[4]. Menaka, Dr. V. Ranganathan, A survey of trust related protocols for mobile Ad-hoc networks, International Journal of Emerging Technology and Advanced Engineering Journal (IJETAR), 3(4), April 2013, 903-910.

[5]. Dr. K. Thirunadana, Sikamani, D. Santhosh Kumar, Efficient and secure trust based ad hoc routing in MANET, Current Trends in Engineering and Technology (ICCTET), 2013, 255-258.

[6]. K. Govindan, P. Mohapatra, Trust computations and trust dynamics in Mobile ad hoc networks: a survey, IEEE Communications Surveys and Tutorials 14, 2012, 279-298.

[7]. G.M. Kaur, K. Kumar, QoS Routing Protocols for Mobile Ad-hoc Networks: a Survey, IJWMC 5, 2012, 107-118.

[8]. P. V Krishna, V. Saritha, et. al, Quality of service enabled ant colony-based Multipath Routing for Mobile Ad-hoc networks, IET Communications 6, 2012, 76-83.

[9]. A Menaka Pushpa, Trust based Secure routing in AODV routing protocol', Published in IEEE, Page 1-6, 2009.

[10]. S. Lu, L. Li, and K. Yan Lam, L. Jia, SAODV: A MANET routing protocol that can withstand Black Hole attack, Published in IEEE ICCIS, 2009, 421-425.

A. Khokhar, L.Abusalah, M Guizani, A survey of secure mobile ad-hoc routing protocols, IEEE Communication in Surveys & Tutorials 19, 2008, 78-93.

[11]. A. Pirzada, A Datta, C McDonald, Incorporating trust and reputation in the DSR protocol for dependable routing, Elsevier, Science Direct, Computer Communications & SCSSE,29, 2005, 2806-2821.

[12]. C Liu, J. Kaiser, A survey of Mobile ad hoc network routing protocols, University of Magdeburg, 2005, 1-36.

[13]. L Khelladi, D Djenouri , N Badache, A survey of security issues in mobile ad hoc and sensor networks, IEEE Communication Surveys and Tutorials, 2005, 2-28.

[14]. Wendi, L Chen, B Heinzelman, "QoS-aware routing based on bandwidth estimation for mobile ad hoc networks", Published in IEEE Communication, 2005, 561-572.

[15]. A Perrig, Y hu, A Survey of secure wireless ad-hoc routing, IEEE Computer Society, 2, 2004, 28-39.

[16]. Y C Hu, A Perrig, and D B Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, 8th Annual IICMCN, Mobicom, 2002, 12-23.

[17]. S. Chakrabarti, Amitabh Mishra, QoS issues in ad- hoc, Wireless Networks, Published in IEEE Communications, 2001, 142-148.

[18]. K Lai, S Marti, M Baker, Mitigating routing misbehavior in mobile ad hoc network, published in Proceedings of 6th annual ACM and IEEE, 2000, 255-265.

[19]. Rinzboorg, N. Asokan, Key Agreement in ad hoc networks, Published in computer Communication, 23, 2000, 1627-1637.

[20]. Praveen Kumar,B Bharath Bhushan, P Chandra Sekhar, N Papanna, A survey on MANET Security Challenges and routing protocols, IJCTA, 4, 2014, 248-256.

[21]. P. Zimmermann, the official PGP Users Guide, MIT Press, 1995.

[22]. N. Bhalaji, A. Shanmugam, Dynamic Trust based method to mitigate Grey hole Attack in Mobile Ad-hoc Networks, Published in Procedia Engineering, 2012, 881-888.

[23]. Rajshekhar Tiwari and Manish Sharma," Comparative Analysis of Trust based and Intrusion based black hole prevention in AODV in MANET, IJCNWMC, 4, 2014, 151-158.