Trust Based Routing Approach to Enhance Received Data Packets by Various Nodes in MANET

Vijay Kumar Singh[1], Piyush Kumar Shukla[2], Sachin Goyal[3]
[1]Dept. of CSE, Bansal College of Engineering, Mandideep, Bhopal (M.P.) India.
[2,3] UIT, RGPV, Bhopal (M.P.) India.

ABSTRACT
In this paper, Trust prediction has been used for checking the trustworthiness of the nodes present in the network. Trust prediction finds the best route for the routing that is free from malicious nodes. DTQR (Distributed Trust based QoS aware routing) is based on AODV (Ad-Hoc on Demand Routing) protocol. We compare the DTQR (Distributed Trust based QoS aware Routing) algorithm with TQR (Trust based QoS aware AODV 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 has been improved.

Keywords - Trust prediction, trust degree, Watchdog, AODV, 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 dynamic change in topology, the routing of data is promising.

Ad-hoc networks have various applications such as in healthcare application, military applications. Battle-field applications where wired connection 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.

Base on Trust every node contains a pair of public and private keys in Public Key Infrastructure. Public keys are common that is distributed 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.

II PROPOSED METHODOLOGY

When sender node (T) wants to communicate with the destination node (R), Transmitter node T checks whether a path to destination node is available.

Step 1: if the legitimate path exists to the destination node then the nodes present in the route must meet the requirements i.e. trust and QoS constraints. If a trusted route exists then go to step 3. If a trusted route is not found, then the sender node initiates a route discovery process using DTQR protocol.

Step 2: While mobile nodes are in the range of network, then node S broadcasts RREQ packets to its intermediate nodes.

Step 3: Each intermediate node (I) is watched by the neighbor nodes Ng and set the suspicious nodes (S)

Step 4: While suspicious nodes (S) is not a receiver then the trust value of suspicious nodes is calculated.

Step 5: If receiver is a suspicious node present in the network, then send acknowledgement to the sender and start data forwarding otherwise receiver is not present in the network range.

Step 6: When the data forwarding is started,

Step 7: If the trusted path exists go to step 9.

Step 8: Else set the nodes as suspicious nodes in the path, and neighbor nodes watch the suspicious nodes.

Step 9: When the packet is sent through the sender, then

Step 10: If suspicious nodes are receiving the packet but does not forward the packets to the next node else go to

step 12.

Step 11: Decrease the trust value by:

$$\text{New\_trust} = \text{S\_old\_trust} - \frac{\text{Number of packets forwarded by a node}}{\text{Number of packets received by a node}}$$

And set new trust value for S.

Step 12: Increase the trust value by:

$$\text{New\_trust} = \text{S\_old\_trust} + \frac{\text{number of packets forwarded by a node}}{\text{number of packets received by a node}}$$

And set new trust value for S.

Step 13: All neighbor nodes calculate the trust value for each node separately.

Step 14: neighbor nodes send trust report to the trust calculator node.

Step 15: trust calculator node D calculates the average trust value for all suspicious nodes (S).

Step 16: While count is less than equal to 2 that is count<=2 , the trust value of suspicious nodes is calculated.

Step 17: Increment count

Step 18: When count=2 and trust value is less than 0.5 then go to step 19 else go to 20.

Step 19: Block the suspicious nodes and set the node as attacker.

Step 20: Enter the suspicious node in the trusted group.

Step 21: the packet delivery ratio is calculated.

$$\text{PDR} = \frac{\text{Number of packets received by a node}}{\text{Number of packets sent by a node}} * 100$$

Step 22: Time Duration of Packet= End-Start;

Step 23: If packet duration is greater than zero then

Step 24: Sum= Packet_duration + Sum

Step 25: Increase the received num i.e. recvnum++

Step 26: Calculate Delay as

$$\text{Delay} = \frac{\text{sum}}{\text{recvnum}}$$

Step 27: Calculate the percentage of malicious attack

$$\text{malicious attacks } \% = 100 - \left(\frac{\text{msends}}{\text{tsend}}\right) * 100$$

Where, msends= packets sent through malicious or mistrusted nodes
Tsend= packets sent through trusted nodes

III 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 shows the simulation parameters that have been used in the mobile ad-hoc network for performing the simulation. The performance is analyzed in the network and values have been tabulated.

We have compared 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 it is used for detecting the malicious nodes in the network.

Table 1
Table of simulation parameters

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

Table 2:
Table of Send Data Packets

Time (in Secs)	Sent Data Packets
0	0
150	7493.00
300	15112.00
450	22732.00
600	30350.00
750	37969.00
900	45589.00

Table 3:
Table of Send Data Packets by Various Nodes

Time(in secs)	Received Packets by Nodes		
	DTQR	TQR	Watch Dog- DSR
0	0	0	0
150	3375.00	2997.00	2699.00
300	8884.00	8247.00	7587.00
450	17246.00	15095.00	13579.00
600	25192.00	21110.00	19792.00
750	33687.00	32721.00	27809.00
900	44115.00	42120.00	32949.00

Source nodes send data packets to the destination nodes through routing protocols. In the table 2 & 3, 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.

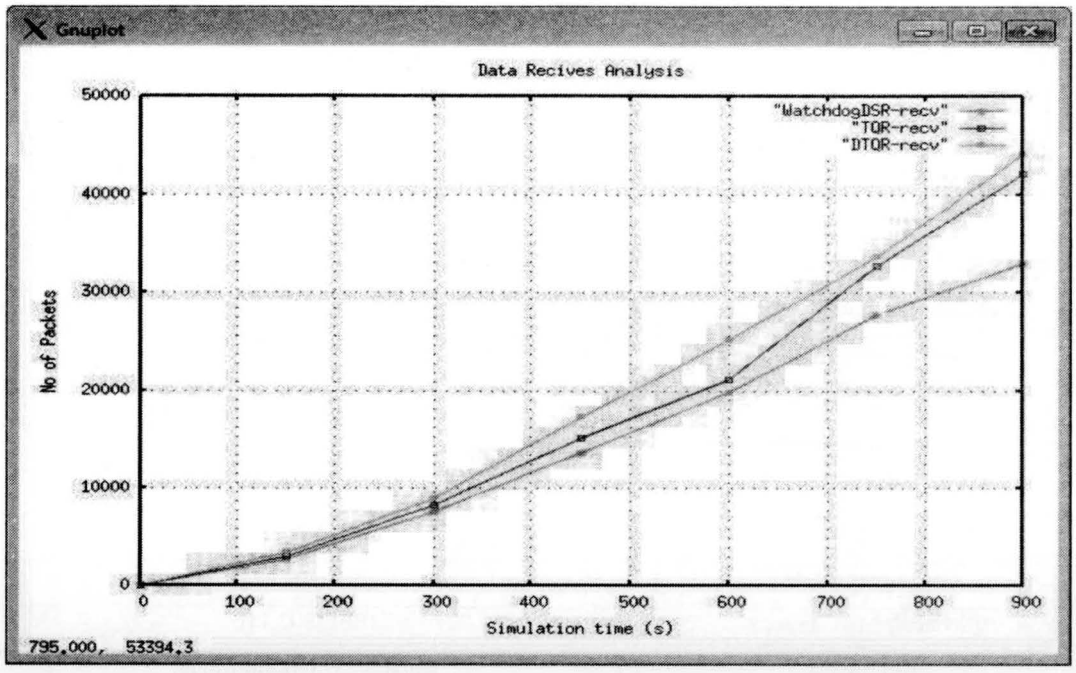

Fig 1: Variation of Data receiving analysis

IV SIMULATION RESULTS

Figure 1 shows variation in data receiving packets. DTQR shows better performance than Watchdog-DSR and TQR.

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 distributed 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.

V CONCLUSION

In the proposed work, a trust mechanism based on Ad-Hoc on Demand Routing protocol termed as DTQR (Distributed 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.

Distributed 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, end-to-end delay ratio, packet receiving ratio and routing packet overhead 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] Vijay Kumar Singh, Piyush Kumar Shukla, Sachin Goyal, "Survey of Various Trust Based QoS Aware Routing Protocol in MANET," GJRA - GLOBAL JOURNAL FOR RESEARCH ANALYSIS, Volume-5, Issue-11, November – 2016, pp. 468-470, ISSN No. 2277 – 8160.

[2] Vijay Kumar Singh, Piyush Kumar Shukla, Sachin Goyal, " Dispersed Opinion based QoS Cognizant Routing Protocol against Black hole Attack in MANET, " *IOSR Journal of Mobile Computing & Application (IOSR-JMCA) e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 3, Issue 6 (Nov. - Dec. 2016), PP. 29-37 www.iosrjournals.org.*

[3] Bo Wang, Xunxun Chen, Weiling Chang, "A light-weight trust-based QoS routing algorithm for ad-hoc networks," Pervasive and Mobile Computing, Elsevier, June 2014, pp. 164–180, www.elsevier.com/locate/pmc.

[4] N. Marchang, R. Datta, Light-weight trust-based routing protocol for mobile ad hoc networks, IET Information Security 6 (2) (2012) 77–83.

[5] Jing-Wei Huang, I. Woungang, Han-Chieh Chao, et al. , "Multi-path trust-based secure AOMDV routing in ad-hoc networks, " IEEE Globecom, 2011, Kathmandu, Nepal.

[6] Zhi Li, Xu Li, V. Narasimhan, "Auto regression models for trust management in wireless ad hoc networks, in: IEEE Globecom, 2011, Kathmandu, Nepal.

[7] Bo Wang, Chuanhe Huang, Layuan Li, et al., "Trust-based minimum cost opportunistic routing for Ad hoc networks, " Journal of Systems and Software, 84 (12) (2011) 2107–2122.

[8] Jian Wang, Yanheng Liu, Yu Jiao, Building, "A trusted route in a mobile ad-hoc network considering communication reliability and path length, " Journal of Network and Computer Applications 34 (4) (2011) 1138–1149.

[9] Jian Wang, Yanheng Liu, Yu Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length, " Journal of Network and Computer Applications 34 (4) (2011) 1138–1149.

[10] Jeffery P. Hansen, Hissam Scott, Plakosh Daniel, Wrage Lutz, "Adaptive quality of service in ad-hoc wireless networks, " IEEE Wireless Communications and Networking Conference (WCNC) (2012) 1749–1754. WCNC 2012.

[11] Zae-Kwun Lee, Gyeongcheol Lee, Hyung Rai Oh, Hwangjun Song, "QoS-aware routing and power control algorithm for multimedia service over multi hop mobile ad-hoc network, " Wireless Communications and Mobile Computing 12 (7) (2012) 567–579.

[12] Kunavut Kunagorn, Sanguankotchakorn Teerapat, "Generalized multi-constrained path (G_MCP) QoS routing algorithm for mobile ad hoc networks, " Journal of Communications Vol. 7, No. 3, (2012), pp. 246–257.

[13] P. Venkata Krishna, V. Saritha, G. Vedha, et al., "Quality-of-service-enabled ant colony-based multipath routing for mobile ad-hoc networks, " IET Communications, Vol. 6, No. 1, (2012), pp. 76–83.

[14] Kajioka Shinsuke, Wakamiya Naoki, Satoh Hiroki, et al., "A QoS-aware routing Mechanism for multi-channel multi-interface ad-hoc networks," Ad-hoc Networks, Vol. 9, No. 5, 2011, pp. 911–927.

[15] E. Ghadimi, A. Khonsari, A. Diyanat, M. Farmani, N. Yazdani, " An analytical model of delay in multi-hop wireless ad hoc networks, " Wireless Networks Vol. 17, No. 7, 2011, pp. 1679–1697.

[16] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, et al., " Trust management in mobile ad hoc networks using a scalable maturity-based model, " IEEE Transactions on Network and Service Management, Vol. 7, No. 3, 2010, pp. 172–185.

[17] Priya Kautoo, Piyush Kumar Shukla, Sanjay Silakari, "Trust Formulization in Dynamic Source Routing Protocol Using SVM, ", International Journal of *Information Technology and Computer Science (IJITCS),MECS, Hong Kong, July,* 2014, pp. 43-50, (http://www.mecs-press.org/) DOI: 10.5815/ijitcs.2014.08.06.

[18] Priya Kautoo, Piyush Kumar Shukla, Sanjay Silakari, "Inclusive Survey of Various Trust based Dynamic Source Routing Protocol for Mobile Ad-hoc Network," International *Journal of Computer Applications (0975 – 8887) Volume 93 – No 4, May 2014,* pp. 7-12.

[19] Jyoti Verma, Piyush Kumar Shukla, Rajeev Pandey, "Survey of various Trust based QoS aware Routing Protocol in MANET, " *International Journal of Computer Applications (0975 – 8887) Volume 137 – No.3, March 2016, pp. 34-43.*

[20] The network simulator - ns-2, http://www.isi.edu/nsnam/ns/, 2012.