www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -02 February , 2016 Page No. 15657-15660

Review: Performance Estimation of Best Ad Hoc Routing Protocol with Trust Mechanism in MANET

Anil Kumar[1], *Gaurav Banga*[2]

[1] M.tech Scholar, Electronics and Comm. Deptt. Geeta Institute of Management and Technology, Kurukshetra University,
Kurukshetra, Haryana, India
Anildhamada29@gmail.com

[2] Assistant Professor, Electronics and Comm. Deptt. Geeta Institute of Management and Technology, Kurukshetra University,
Kurukshetra, Haryana, India
Gauravbanga86@gmail.com

ABSTRACT: ***A MANET is a type of ad-hoc network that consists of wireless mobile nodes communicates with each other without using wires, a fixed infrastructure, central administration and which establishes route from source to destination. In Mobile Ad-hoc Network (MANET), each node can freely move in any direction and every node also act as router as they forward traffic for other nodes. So, various routing protocols such as AODV, DSR, DSDV and OLSR are designed for routing in ad-hoc networks. This paper analyzed the literature of routing protocols which are discussed by comparing the various routing protocols on the basis of different schemes.***

I.INTRODUCTION:

In MANETs, Ad-hoc means '*for this purpose*' which comes from Latin word. In ad-hoc network, the medium is wireless which is designed to replace the wired infrastructure. The movement of nodes is the terminal that is involved in an ad-hoc network which is generally known as Mobile Ad-hoc Network (MANET).

In Mobile Ad-hoc Networks each node can move randomly in Omni-directional manner and forward packets to find or establish the route from source node to destination node. In MANET, every node can join or leave the communication route network easily and changes network topology repeatedly due to high mobility of nodes. Therefore, routing becomes a difficult task in ad-hoc networks. Many routing protocols have been anticipated for ad-hoc networks such as AODV, DSR, DSDV, OLSR etc which is based on design goals of minimum control overhead, multiple hop routing capability, topology allowance and loop avoidance. Hence routing protocols perform four important functions as determination of network topology, retaining network connectivity, channel requirement and transmission forecasting and packet routing.

Several aspects which affect the global network performance of routing protocols functioning in ad-hoc networks such as size of network, traffic strength and control overhead. The performance metrics i.e. End-to-End Delay (EED), Throughput, Control Overhead, Packet Delivery Ratio (PDR) and Normalized Routing Load (NRL) helps to distinguish the network that is affected by routing aspects that may control performance of network.

II.AD-HOC ROUTING PROTOCOLS: Routing protocols in ad-hoc networks can be categorized on routing strategy wise or network structure wise. In accordance with routing strategy wise, routing protocols can be classified as proactive or table-driven protocol and on-demand or reactive routing protocol. Both these techniques can be evaluated from its performance metrics. In this paper, AODV and DSR are the examples of reactive protocol and DSDV and OLSR are the examples of proactive protocol.

Ad-hoc On-demand Distance Vector (AODV):

As name indicates AODV is a combination of on-demand and distance vector i.e. node-to-node routing or hop-to-hop routing approach. AODV protocol determines route discovery using control messages as RREQUEST and RREPLY. In AODV, routes are established by submerging the network with RREQUEST packets from source to destination. The RREQUEST is dispatched by intermediate nodes and these intermediate nodes also makes inverse route for itself for destination. The destination node makes a RREPLY when RREQUEST arrives to destination. The RREPLY includes the number of hops which requires arrive to the destination. All nodes that onward the RREPLY to source node produce forward route from source to destination. So, discovery of route from source node to destination node is a hop-by-hop state.

Dynamic Source Routing (DSR):

DSR is also an on-demand routing protocol. The DSR protocol consists of two techniques that work together to permit the discovery and continuance of source routes in ad-hoc network. Route Discovery is the technique by which a source node desires to forward a packet to a destination node and find a resource route from source node to destination node using RREQUEST and RREPLY messages. Route Continuance is the technique by which a source node is capable to discover while using resource route to destination node if the network topology has altered because a linkage alongside the route no longer works. When route continuance specifies a source route is destroyed, DSR forwards RERROR message to source node for obtaining a new route.

Destination Sequenced Distance Vector (DSDV):

DSDV is a hop-by-hop distance vector routing protocol which is based on the idea of classical Bellman-Ford routing algorithm. In this algorithm, each node uphold a routing table like distance vector, which it exchanges with its neighbour nodes, record the "next hop" for each nearby destination, number of hops to arrive destination and the sequence number allocated by destination node. The sequence number is applied to discriminate routes from new ones and thus reduces loop configuration. Two types of routing table exchanges are used as: time-driven and event driven updating.

Optimized Link State Routing (OLSR):

OLSR is a proactive routing protocol which uses the idea of MPR (Multi Point Relays) for onward control traffic. OLSR is an optimization of real link state algorithm. Two types of control messages like Hello messages and Topology Control messages are used in OLSR. Hello messages are utilized for obtaining the information about the level of the linkage and node's neighbours. Topology Control (TC) messages are utilized for propagating information about its own publicized neighbours.

III.PERFORMANCE METRICES:

1. Average End-to-End Delay (EED): It is defined as the time taken for a complete message to broadcast from source to destination. It depends on the broadcasting time, communication time, queuing time and dispensation delay.
2. Normalized Routing Load (NRL): It is the number of data packets spread by routing protocols as per data packet carried at the destination.
3. Packet Delivery Ratio (PDR): It is the ratio of number of data packets effectively received to the destinations from source to destination.
4. Throughput: It is the average rate of successfully broadcasted data packets in a unit time over a communication channel.
5. Control Overhead: It is the ratio of control information transmitted to the actual data received at each node.

IV.LITERATURE REVIEW

There are various schemes used to compare and find best routing protocol from various routing protocols:

A proximity-based dynamic path shortening scheme, called DPS in which on the basis of local link quality estimation at each own node, find active route paths dynamically to node mobility without exchanging control packets such as Hello packets. In DPS, each node monitors its own local link quality only when receiving packets and estimates whether to enter the 'proximity' of the neighbour node to shorten active paths in a distributed manner. Simulation results of DPS in scenarios of various node mobility and traffic flows reveal that adding DPS to DSR and AODV reduces end-to-end packet latency up to 50 percent and also number of routing packets up to 70 percent, in heavy traffic cases [1].

The four performance measures i.e. end-to-end delay, PDR, throughput and control overhead with different number of nodes, different speed of nodes and different size of network are used for analysis the performance of AODV, DSR, DSDV and OLSR protocols. AODV and DSR protocols are the best in terms of average PDR. AODV and DSR give better packet delivery ratio than other protocols if network size is less than 600x600sqm. If the network size is more than 600x600sqm, the OLSR protocol is the better solution for high mobility condition [5].

The performance of reactive routing protocols, AODV, DSR and DSDV is analyzed with respect to average end-to-end delay, packet delivery fraction (PDF), normalized routing load (NRL) and throughput under the impact of high mobility. The simulation results verify that AODV performs better in a network with large number of nodes as compared to DSR and DSDV [6].

The performance evaluation of routing protocols under different performance metrics like PDF, average end-to-end delay, NRL, packet loss, throughput and routing overhead in different network sizes. The comparison result shows that AODV performs better than DSDV and DSR in terms of PDF and Throughput. DSR gives lowest packet loss and DSDV gives NRL, end-to-end delay and routing overhead than AODV and DSR [8].

The performance of three MANET protocols i.e. AODV, DSR, and DSDV are estimated under three different environments i.e. TCP, UDP and SCTP. Throughput for packet loss and for receiving packets of all routing protocols is tested. From the simulation results, the performance of AODV is very high than DSR and DSDV. The performance of TCP is better than the SCTP and UDP [14].

A trust model which maintains reliability through collaboration instead of achieving trust through security, applied to the secure routing protocols as AODV, DSR and TORA with cryptographic algorithms require many mechanisms like establishment, maintenance and operational mechanisms. The nodes are dependent upon the trusting nature of the other nodes in ad-hoc network. All nodes independently execute this trust model and take decisions about other nodes in the network. The simulation result shows that the trusted TORA protocol performs well in the presence of malicious nodes under low traffic conditions and diverse mobility [7].

An AODV_SQ (Ad-hoc On-demand Distance Vector link Stability Quality of service) protocol which adopts back-up route mechanism and take bandwidth as QOS (quality of service) parameter. Testified by simulation, this protocol gives better improvement in the rate of packet transmission, time delay and route expense relative to AODV [2].

AODV protocol is based on minimum delay path as route selection criteria, find the route before starting send packets, creates the routing table and the topology on on-demand basis, issue the control signal to establish and maintain paths, which could reduce the cost of producing the path, saving a certain amount of network resources, but drawback is to send data packets. The routing of blindness, results in some of the routing node congestion and delays or even data loss and other issues. The simulation results show that the improved AODV protocol in terms of throughput and network delay, especially in higher network load [3].

Wormhole attacks are the powerful attacks in which a malicious node records data packets in the network, which retransmits them into the network locally to another malicious node far away. A modified wormhole detection AODV protocol is introduced to detect wormhole attacks using number of hops in different paths and delay of each node in different paths from source to destination [11].

The characteristics of ad-hoc network with high of mobility, no fixed infrastructure and no central administration makes network more vulnerable to attack. Active attack i.e. blackhole attack and DOS attack can easily occur in ad-hoc network, which decrease the performance of routing protocol. A new trust mechanism, called Trust AODV has proposed to secure the AODV protocol. An ant algorithm is used to improve the performance of proposed secure protocol in terms of packet delivery ratio and throughput [16].

AODV routing protocol is one of the basic protocol that is modified to cope with security demands. An analytical model is used to evaluate the performance of AODV that is developed to be secure with trust mechanism and malicious node detection. Based on analytical model, the performance of proposed protocol which informs a secure route depends on the total nodes in network, topology of the nodes, distance between the source and destination node, total malicious node, the probability of the node to execute malicious attacks and route establishment may fail due to node's movement. The analytical model aims to provide the performance of proposed protocol in the form of route establishment probability of the network with and without malicious nodes [17].

V. CONCLUSION

After analyzing the literature of routing protocol, it is concluded that the most of the researchers had worked on distance based approach for the route selection recently the area is bit diverted as the user need the security to send the data from one place to another. So by considering this some researchers worked on trust value calculation and detection of nodes which are attacker or malicious so as a future scope inspired from those algorithms. The routing protocols can be updated by trust evaluation algorithms and select the route on behalf of trust level of the nodes in network.

REFRENCES

[1] Masato Saito, Hiroto Aida, Yoshito Tobe, Hideyuki Tokuda, "*A proximity-based dynamic path shortening scheme for ubiquitous ad-hoc networks*", IEEE ICDCS'04 1063-6927/2004.

[2] TU Jun , T LUO Zheng-jun, SUN Yun , "*The Research of Routing Protocol in Ad Hoc Network - A kind of modified protocol based on AODV protocol", IEEE 2009 .*

[3] Zhu Qiankun, Xu Tingxue, Zhou Hongqing, Yang Chunying, Li Tingjun*, "A Mobile Ad Hoc Networks Algorithm Improved AODV Protocol",* 2011 International Conference on Power Electronics and Engineering Application (PEEA 2011) ELSEVIER Procedia Engineering 23 (2011) 229 – 234.

[4] Mou Zonghua, Meng Xiaojing, "*A Modified AODV Routing Protocol Based on Route Stability in MANET" 2011.*

[5] S. Mohapatra, P.Kanungo, "*Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator*", International Conference on Communication Technology and System Design 2011. Procedia Engineering 30 (2011) 69 – 76 ELSEVIER.

[6] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey, "*PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS***"**, IJDPS Vol.2, No.6, November 2011.

[7] A. Sudhir Babu, K. V. Sambasiva Rao, "*Enhancement of Performance by Embedding Trust Model into Reactive Routing Protocols (Applied to AODV, DSR and TORA)*", IEEE 2012.

[8] Ginni Tonk, S.S. Tyagi, "*Performance of Ad-Hoc Network Routing Protocols in Different Network Sizes",* IJITEE ISSN: 2278-3075, Volume-1, Issue-2, July 2012

.

DOI: 10.18535/ijecs/v5i2.1

[9] Deepthy Mathew, Shyama Sudarsan, S. Kannan, Dr. S. Karthik, "*A Secure and Energy Enhanced Protocol for Routing in Mobile Ad-Hoc Networks*", IJSER Volume 3, Issue 11, November-2012.

[10] Jogendra Kumar, "*Comparative Performance Analysis of AODV, DSR,DYMO,OLSR and ZRP Routing Protocols in MANET Using Varying Pause Time*", IJCCN, 2(3), pp 43–51, 2012.

[11] Umesh kumar chaurasia, Mrs. Varsha singh Member(IEEE), "*MAODV:Modified Wormhole Detection AODV Protocol*", IEEE 2013.

[12] Sheng Liu, Yang Yang, Weixing Wang , "*Research of AODV Routing Protocol for Ad Hoc Networks*," Conference on Parallel and Distributed Computing and Systems AASRI procedia 2013(21-31) ELSEVIER.

[13] M.Vanitha, Dr.B.Parvathavarthini, "*Performance Analysis of an Enhanced DOA for Mobile Ad-hoc Networks*", IEEE ICSSS March 28 - 29, 2013.

[14] B.Suvarna, K V Krishna Kishore, G.P arimala, R.Prathap Kwnar, "*Performance Estimation of DSR, DSDV and AODV in TCP, UDP and SCTP*", IEEE ICROIT 2014.

[15] A. Komathi, Dr. M. Pushparani, "*Trust Performance of AODV, DSR and DSDV in Wireless Sensor Networks*", IEEE ICCTET 2014.

[16] Harris Simaremare, Abdelhafid Abouaissa, Riri Fitri Sari, Pascal Lorenz, "*Performance analysis of optimized Trust AODV using ant Algorithm*", IEEE ICC 2014- Communications Software, Services and Multimedia Applications Symposium.

[17] Ruki Harwahyu, Harris Simaremare, Riri Fitri Sari, Pascal Lorenz, "*Performance Estimation of AODV Variant with Trust Mechanism",* IEEE ICC 2014 - Ad-hoc and Sensor Networking Symposium.