DYNAMIC SECURE ON DEMAND DISTANCE PROTOCOL FOR MANET

A Sivakumar Chellappan[1], Dr .T. Nalini[2]

[1] *Research scholar, Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai -600073*

[2]*Professor, Computer Science and Engineering, Dr Mgr Educational research and institute ,Chennai- 600095*

Abstract: Mobile Ad Hoc Networks (MANETs) is a gathering of mobile nodes with a dynamic (changing) topology and it works under versatile conditions for some applications and cause different security contest. Perceiving the trouble making is a dreary issue, in light of the nomadic idea of nodes. For perceiving the destination route, nodes will share the routing subtleties between the neighbors. Along these lines, nodes should trust each other, and here, trust is the primary concern in secure routing instrument. AOSR protocol is proposed in our work by expanding the AODV protocol, which works as indicated by the novel trust instrument, an improved appropriated trusted secure routing protocol. Here, in light of the trust estimations of its neighbor nodes, the node chooses the routing choice. What's more, finally, proposed technique adjusts the traditional AODV routing protocol with the limitations of trust rate, energy, and mobility., as per the malicious conduct expectation. The trust rate is characterized by the packet grouping ID coordinating from the log reports of neighbor nodes, which takes out the malicious report generation. The trust level is expanded by utilizing the immediate and roundabout trust perception plans. The trusted node is checked whether it is inside the communication go or not, with the assistance of received sign quality pointer. From the test result it is affirmed that the AOSR can evade the malicious nodes viably when assembling the route; in addition, it additionally achieves the better exhibition when contrasted and TSDRP and DTMAC as for throughput, packet delivery ratio, and normal start to finish delay.

Key words: Mobile ad-hoc network (MANET), AODV, Trust management, Secure Routing

1. Introduction

A mobile ad hoc network (MANET) is a wireless network with a high of mobility, autonomic, temporary, no fixed infrastructure and no focal administration. It is broadly utilized in military system, common crisis search, salvage operations and different events. Nodes in the network generally have restricted resources, for example, processor, bandwidth, memory, and energy. In traditional wireless networks, a base station or access point encourage communications between nodes inside or outside the network [70]. Conversely, MANET is an infrastructure-less network where each node goes about as a router for setting up the association between sources to destinations. In MANET [1], every node can move in an arbitrary way and forward the packet communication between one another to discover or set up the communication route to the destination node. Each node that partakes in the network is answerable for the solid operation of the entire network. MANET topology may change quickly and erratically because of the high mobility of the nodes. At the point when the network topology is changing, the associations should be restored. In addition, the features of ad hoc networks are like ordinary wireless network. All the characteristic practices in wireless ad hoc network cause security issue to turn out to be more perplexing. A portion of the MANET characteristics are: there is no administrative node to control the network, open network and each node can partake in the network without any problem. These qualities make MANET more vulnerable to an adversary's malicious attacks. Numerous potential attacks can be acted in every communication layers. In ad hoc network, dynamic assault for example DOS, and blackhole assault can undoubtedly happen. These attacks could diminish the presentation of the routing protocol. Routing protocols in MANET can be arranged into three kinds dependent on the routing data update system for example responsive protocol, proactive protocol and half and half protocol [4]. The advantage of receptive methodology when contrasted with proactive routing is that it acquires lower calculation expenses and lower packet overhead since nodes are not needed to trade routing data intermittently to keep up route tables. Some of routing protocols under this idea are DSR [13], TORA [1], and AODV [12].

AODV has preferable execution over the others responsive routing protocols [4]. It offers snappy adaptation to dynamic link conditions, low handling, low memory overheads, and low network usage [29]. In term of security, there are two principle systems to upgrade the security of AODV routing protocol for example cryptographic system and trust based instrument. Both of these instruments have an alternate way to deal with secure the network communications. Cryptographic system use encryption strategy, public key technique or another's cryptographic strategy to ensure the packet

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

communication. Anyway trust component figures the trust level of every node before setting up the communication. Trust level is characterized from the conduct boundaries of the network or nodes. Contrasted with the cryptography component, the trust has a superior exhibition as opposed to cryptography system [58]. Secure routing protocol utilizing cryptography strategy has a few disadvantages for example to begin with, there are noteworthy network overhead because of the additional data traded. Second, addressing the potential for malicious suggestions requires a trusted outsider or a computationally costly public key infrastructure, which conflicts with the self-association nature in MANET. Something else, trust component doesn't need for mentioning and checking authentications security constantly, and doesn't need the addition header in the packet to secure the communication cycle, for instance private or public key. These can improve the presentation of routing protocol. In light of these affirmations, this part addresses to propose a secure AODV routing protocol utilizing trust system. The proposed protocol is called Trust AODV. It is assessed utilizing NS-2 under attacks. We pick these attacks because of these attacks can diminish the network execution altogether. The exhibition of AOSR will be contrasted and the comparative secure protocol for example TCLS [49].

The rest of the paper is organized as follows: Sect. 2 explains related works to Secure routing. Section 3 discusses proposed method used to find Secure path in MANET. Section 4 illustrates the evaluation of the proposed method. Section 5 we conclude the paper.

2 RELATED WORKS

In Ad hoc composes, utilizing the trust and picking an accepted course for package transmission is a gigantic component. Seeing the malicious center points in the method of guiding and to evade the enemies from publicizing themselves as extraordinary is the goal of trust establishment instrument. For secure controlling, various authorities proposed particular trust appraisal models. Here, we explain the unmistakable Routing show in MANET and perceive among three shows as Reactive, Proactive and Hybrid, reason of various boundary as coordinating perspective, controlling plans, coordinating overhead, torpidity, and adaptability level.

The detail examination of different guiding attacks in MANET is depicted in [9]. The security is most inquiries in Mobile off the cuff mastermind (MANET) under various guiding attack, because of open nature of flexibility. Future Work centers around Security in MANET and gives a security under various attacks. The security is pressed in [7], with the help of different cryptography strategy for security and perceive among the symmetric figurings, for instance, AES and Blowfish and Asymmetric computations like RSA and ECC used for confirmation. The yield says that: ECC (Elliptic twist Cryptography) is better than RSA. The other security techniques in Cryptographyis explained further. The distinctive coordinating shows in MANET and diverse Routing attacks in MANET with various security plans, was portrayed in [].

Unmistakable kind of guiding attack present in the MANET as the working of various security shows is explained in this work. We can see the better course of action of such various attacks, using security shows. These security shows were executed in MANET to restrict the effect of the attacks [10]. The trust based security coordinating with trust in various perspectives in MANET was examined in [15]. It is tedious to manage the trust based security in MANET, because of its open nature; it is the basic discussion of MANET. Entire conceivable trust the board for secure coordinating with fundamental shows was investigated here. In order to endorse the assessments of a trust, it enrolls the trust and informal communities.

Viable Trust based directing using troubles to develop security was suggested in [20]. This takes the arrangement from this current reality system of sidekicks. IT will disconnect the noxious center points which are left with no imagine. The standard disadvantage here is: it doesn't rely upon any arrangement that will spread information about the malicious center point so the chances of affecting happens are especially low. The outstanding test is in affirming the center points exceptional attributes. Secure Zone coordinating Protocol (ZRP) was proposed in [2], for seeing the creation inconvenience centers and keep mastermind from destroying. Neighbor Discovery Protocol (NDP) perceives the neighboring centers in the far off station contemplating its zone and round journey information, in MANET. Bundle uprightness is given in Secure Intra Zone Routing Protocol (SIERP), which utilizes the RSA and advanced imprint.

Trust Based Secure On Demand Routing Protocol (TSDRP) was suggested in [3], where the Adhoc on intrigue Distance vector (AODV) is changed to propose TSDRP to confirm it from various attacks like Black hole attack, Denial of administration attack, etc. Nevertheless, this show gives protection from these attacks. In [3], we utilize the segment to see the affecting center points through seeing of the lead of center points and perceive the direct with got reputation regard in an alarm message. As Collude centers are remembered they are discarded for additional correspondence. In order to fulfill the security demands, earlier, DTMAC was proposed, yet disastrously it faces different perils from harmful centers. One and more people from the affecting bundle part need to disturb the system for making sure about the trust based condition against crash attack, which sees the colluders and rebuke them. We can see the colluders and rebuke them by discarding the affecting CH and

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

keep them from additional enthusiasm for the system correspondence by checking the lead of centers.

A friendship based trust based model for secure guiding from source to objective was proposed in [14], to demonstrate the degree of center point reliability we bring the different degrees of connection. This reviews the drawbacks of ignoring the social lead of the pernicious center point. We use predict centers direct for future correspondence, in order to make a translation of the verification in to evaluation. A logical model is incorporated for this trust director. A methodology boss empowers particular decision standards and game plans. Evaluation Trust secure coordinating reliant on trust levels was suggested in [15], which upgrades the bundle movement extent with the help of trust to disengage Black opening attack and offer secure directing for data traffic. In the system, we register the extent if powerful bundle trade among the neighbor center points.

Evaluation trust show will be requested dependent on the hugeness of the trust level of the center, as demonstrated by the extent centers in the system. It continued till the package accomplishes the objective. Uniqueness coordinating with keeping up and supervising of a current isolated security Architecture is influenced and composed, and this idea is explained in [16]. The insect agent put positive pheromone, when the node is trusted. Way communication works as indicated by this pheromone. The presentation improves as for packet delivery ratio and throughput. An algorithm for trust evaluation of each node and trust calculation metric dependent on node's imprudent conduct to became, malicious in unique condition was recommended in [8].

A trust model is characterized which helps in node authentication and it evaluation work assists with estimating the trust esteem dependent on encounters. A trust relationship work was characterized, to consolidate daze trust esteem and referential trust esteem. In this part numerous plans are investigated and studied in MANET for giving the trust based secure routing to guarantee the trust in multiple points of view. Open nature makes it dreary to keep up the trust and resource limitations; thus the trust is the favored test for best execution. Here we analyze the whole plausible trust management for secure routing with essential protocols. The trust to be registered and social networks assists with checking the calculation of trust and it is proper in unique topology, which is assigned to the network like military however with specific imperatives, for example, looking after unwavering quality, scalability, re-configurability.

3 ADHOC ONDEMAND SECURE ROUTING(AOSR)

Adhoc Ondemand Secure Routing (AOSR) is a secure routing protocol dependent on the AODV protocol. The route revelation and route upkeep components depend on AODV and elaborated as follows. Let us accept that a source node S needs to find a route to destination node D. Likewise accept that A, B and C are three moderate nodes on the way from S to D, that their authentications are certA, certB and certC and their private keys are Ka, Kb, Kcrespectively. During the route revelation stage, a source node broadcasts a RREQ packet marked with its public key. The packet contains the destination node's address D, source node's declaration certS, a nonce N and a timestamp t. The nonce and timestamp guarantee that the route is new. A succession of route disclosure messages is demonstrated as follows:

$S \rightarrow * : (RREQ, D, cert_S, N, t) K_s$
$A \rightarrow * : ((RREQ, D, cert_S, N, t) K_s) K_a, cert_A$
$B \rightarrow * : ((RREQ, D, cert_S, N, t) K_s) K_b, cert_B$
$C \rightarrow * : ((RREQ, D, cert_S, N, t) K_s) K_c, cert_C$

As appeared, each moderate node, (for example, A, B or C) that advances the RREQ packet checks the signature(s) of the past node on the packet by extricating the public key from the testament. Further, it eliminates the past node's mark, signs the RREQ packet with its own private key, adds the declaration to the header and broadcasts the packet to its neighboring nodes. This cycle proceeds until the packet arrives at the destination D.

$D \rightarrow C : (RREP, S, cert_D, N, t) K_d$
$C \rightarrow B : ((RREP, S, cert_D, N, t) K_d) K_c, cert_C$
$B \rightarrow A : ((RREP, S, cert_D, N, t) K_d) K_b, cert_B$
$A \rightarrow S : ((RREP, S, cert_D, N, t) K_d) K_a, cert_A$

On getting the RREQ, D will make a route answer (RREP) packet, add the source address S, its own testament certD, a nonce and a timestamp and sign it with its private key. A middle route C on getting the RREP packet will thusly check the signature(s) of the past node. For instance, when node B receives the RREP packet from node C, it will check the mark of node C. It will at that point eliminate C's testament, sign the packet with its own private key Kb, add its declaration certB and unicast it to the following node An on the opposite way as appeared previously. Nodes B and A will likewise add a routing table section to node D demonstrating that the following bounce is C and B separately. At the point when node B finds a wrecked link to C, it starts route support as appeared:

$B \rightarrow A : ((RERR, S, D, certB, N, t) Kb)$

$A \rightarrow S : ((RERR, S, D, certB, N, t) Kb)$

Accordingly it sends a RERR packet, the source node's address, the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

destination address, its own endorsement certB, a nonce and a timestamp marked with its private key to its past node A. Node A will advance this unaltered to the source node S. AOSR forestalls against attacks which alter the routing data since it utilizes public key authentication. Be that as it may, it is vulnerable tasks attacks which flood the network with counterfeit packets because of the utilization of testaments which require high bandwidth and preparing power of nodes.

3.1 ROUTE OPTIMIZATION

The objective is to propose upgraded routing protocol that can speak with infrastructure network. The algorithm to set up the communication of our proposed protocol is practically like R-AODV routing protocol. RREP is supplanted with R-RREQ to fabricate a multipath ways towards the source node. R-RREQ packet is the adjustment of RREQ packet by adding answer time data field in the packet header. Packet RREQ is likewise changed by adding demand time field in the header packet. Configuration RREQ packet is portrayed in Figure 4.1

Type	Reserved	Hop Count
Broadcast ID		
Destination IP address		
Destination sequence number		
Source IP address		
Source sequence number		
Request time		

Figure 3.1 RREQ Packet

Door nodes help the nodes in ad hoc network to have the option to associate with infrastructure network. The position of the entryways is static in the network situation. At the point when a door receives a RREQ, it will analyze the routing table for the destination IP address indicated in the RREQ message. On the off chance that the address isn't discovered, the passage advances the RREQ to the following ad hoc nodes. Then again, if the door finds the destination in its routing table, it will broadcast a RREP as typical, however may likewise alternatively send a RREP_I back to the originator of the RREQ. This will give the mobile node a default route despite the fact that node has not mentioned it. In the event that the mobile node needs to speak with the Internet later, the default route is already settled, and some other tedious entryway revelation cycle can be stayed away from. In the event that middle of the road mobile node doesn't locate a legitimate route to the destination and if the destination is a fixed node, it will make or update route section for the fixed node in its routing table and forward the information packets towards the passage.

Source node broadcasts RREQ packet to all neighbor nodes to discover the route to the destination node. On the off chance that the node which received the RREQ packet isn't the destination node, at that point it advances RREQ to every neighboring node. On the off chance that the destination node receives RREQ, it will check whether the passage mode on. In the event that the entryway mode is on, at that point the packet will be sent to the network infrastructure utilizing door node measure. On the off chance that the passage mode is off, Reverse RREQ (R-RREQ) will be generated and afterward it will broadcast it to all neighboring nodes to discover the source node. At the point when R-RREQ is broadcasted, each node will check again its repetition. On the off chance that R-RREQ has been received, at that point the packet will be overlooked. Else it will be sent to the following node. In the event that RREQ has discovered the source node, the packet transmission between nodes will begin right away. On the off chance that node isn't the destination or not the passage and doesn't have the route, therefore it will send demand door to all neighbor. At the point when a node isn't the destination and doesn't have the route and receives demand message not for the passages, at that point it will advance sending demand. However, in the event that the node is a passage, at that point it will send RREP to tell that the node is an entryway. Figure 3.3 portrays the route disclosure component of AOSR.

3.3 TRUST MECHANISM

In light of the writing learn about the trust system for making sure about the routing protocol, achievement ratio turns into a significant boundary to ascertain the trust level of the nodes. A portion of the proposed trust component utilizes the achievement ratio of packet routing or achievement ratio of packet information or utilizations them two. The point of the trust estimation is to recognize the likely assault and moderate the aggressor to dodge its effect on the network. The trust estimation can just perform after communication is built up, if the packet information is utilized as a boundary. The assault can't be identified by the trust system in the event that it is perform during the route disclosure stages, on the grounds that the nodes just compute the achievement ratio of packet information. In the event that the packet routing is utilized as a boundary to compute the trust level, the trust component straightforwardly begins the detection when the node plays out the route disclosure stages. This permits the trust instrument to moderate the aggressor before the communication is built up. In our trust estimation, we use routing packets as boundaries to ascertain the trust level of every node.

The achievement ratio is the correlation of the contrast between progress packet and bombed packet to the collection of accomplishment packet and bombed packet. In this methodology, we can't distinguish the definite practices of the every node. In the event that the node is a malicious node, there is a likelihood that the malicious nodes just sends or advances a few packets, not all the packets. Nonetheless, the trust level of every node is determined dependent on the correlation between absolute RREQ packet shows up in the destination node to

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

the complete of packets that have been sent by the every node. This methodology just uses the complete number of RREQ packet that shows up in the destination. Each time the middle node advances the routing packet, it will copy the routing packets dependent on the quantity of its neighbors. The absolute number of RREQ packet sent ought to be greater than the complete acknowledged RREQ in that node. With this methodology, we expect that the absolute RREQ in the destination can't be a boundary to ascertain the trust level of every node in the network. Our proposed trust count registers the node trust level dependent on the practices and exercises of every node. The presumptions about the ordinary exercises are:

The node is a typical node on the off chance that it advances all the routing packet to its neighbors. In light of this presumption, the complete number of packet sending must be equivalent or more than the all out packet receives at the nodes. The absolute sent RREQ relies upon the all out neighbors of that is node. b. On the off chance that the immediate neighbor nodes don't receives the packet that have been sent by its neighbors, at that point this nodes is suspected as a malicious nodes. In light of these suspicions, the trust practices estimation is isolated into two sorts of trust for example trust local figuring (TL) and trust global counts (TG). The meaning of trust local and trust global as follows. a. Trust global (TG) is the trust level computation dependent on the complete exercises of the nodes. The exercises are the absolute number of received routing packets and the all out number of sending routing packets.

Trust local (TL) is the node trust estimation dependent on the all out number of routing packets that have been received from a particular node and forward it to its self. Every node in the network will compute the trust local and trust global of its neighbors. The node must gather TL and TG esteems to register the all out trust level of its neighbor nodes before sending or sending the packets.

$$TLi, = \sum Pri, \sum Prifj, ; wherePrifj, k \neq 0$$

$$TGi, = \sum Prj \sum ; herePsj \neq 0$$

Where TLi, is the trust local assessment of node I to node j, TGi, is the trust global assessment of node I to node j, Pr is the received routing packet, Ps is the sent routing packets and $Prifj$, is the all out sent routing packet from node I by the j that inception from node k. Trust local (TL) is the correlation of packet routing from the particular nodes. It surveys the particular practices of every node. In AODV, the indistinguishable routing packet is received just a single time by the nodes. Since each time node receives the routing packet, the packet id will be checked. In the event that the packet has been received previously, at that point the most recent one will be overlooked. In view of this suspicion, the node is a typical node if the trust local computation is equivalent to 1. Something else, the node is suspected as a malicious node. In the event that the node is a trusted node, at that point the TL esteem is set 1. Something else, the TL esteem is set to 0. Trust global (TG) is the examination between absolute routing packets that have been received and all out routing packet that have been sent by the node. This shows the global practices of the nodes. In the AODV protocol, routing packet will be sent if the transitional node isn't a destination node. The transitional node advances the routing packet to every one of its neighbors. In view of this condition, the complete number of sent routing packet by the node is more noteworthy than the absolute of routing packet that has been received. Accordingly, in the trust global view, the node is an ordinary 101 node if the trust global count equivalent or less than 1. Something else, the node is suspected as a malicious node. In the event that the node is a trusted node, at that point the TG esteem is set 1. Something else, the TG esteem is set to 0. Nodes close the all out trust level of its neighbor by amassing the trust local and trust global qualities. The node is set apart as a trusted node when both outcome assessments collection of TL and TG is trusted. On the off chance that one of the trust feelings is untrusted, the node is suspected as a malicious node. In light of this suspicion, the AND rationale is utiilized to amass the trust supposition esteems. Trust instrument count utilizing TL and TG technique can be performed just if all the nodes in the network can hear all the exercises of its neighbors. To satisfy this condition, the network must be in the wanton mode.

4. EVALUATION

The ns-2 simulator was utilized for the analyses. We presently portray the traffic design, the situation depiction and the measurements that were utilized for the tests. The traffic design document was generated and the boundaries utilized were as per the following In this part, the exhibition of the proposed AOSR approach and the current trust put together routing instrument with respect to non-agreeable condition of MANET, TSDRP [] and DTMAC []. The measurements utilized for the exhibition evaluation of the proposed AOSR approach and existing methodologies are PDR, throughput, normal delay and false positives. The proposed system is reproduced with the network simulator-2 (NS-2) with the simulation boundaries of Table 4.1

Table 4.1: Traffic pattern

Type of traffic	Constant Bit Rate
Packet Size	512 bytes
Packet Rate	4 pkts/sec
Maximum number of	20
Dimensions	2000*2000
Mobility Model	Reference Point Group

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

No. of nodes	10-500
Min. speed	1 m/s
Max. speed	5 m/s
Average number of nodes in a	10
Probability of group change	0.01
Pause time	60 sec

The quantity of nodes was changed from 10 to 500 and the impact on delivery ration, load and Delay was considered. It is discovered that the packet delivery part diminishes as the quantity of nodes in the network increments. This is because of the way that as number of nodes expands, the blockage in the network additionally increments and consequently the quantity of lost packets because of retransmission likewise increments. Further, since AOSR utilizes a table driven methodology, the preparing delay at the nodes additionally increments with an expansion in the size of the network subsequently representing the better quality to-end delay. The standardized routing load increments with an expansion in number of nodes because of an increment in the routing packets in the network.

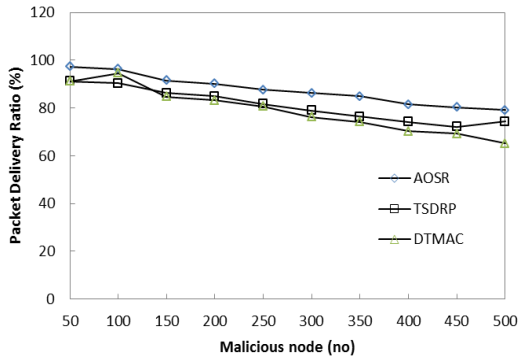

Fig.4.3 Packet Delivery Ratio

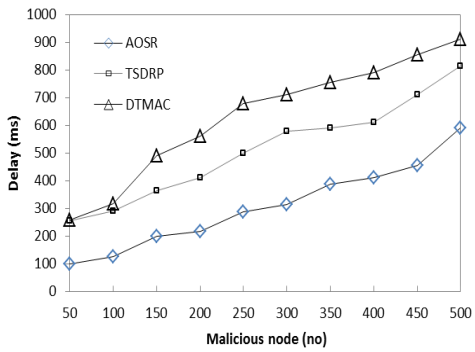

Figure 4.4: Effect of varying the number of nodes on the Average end-end delay

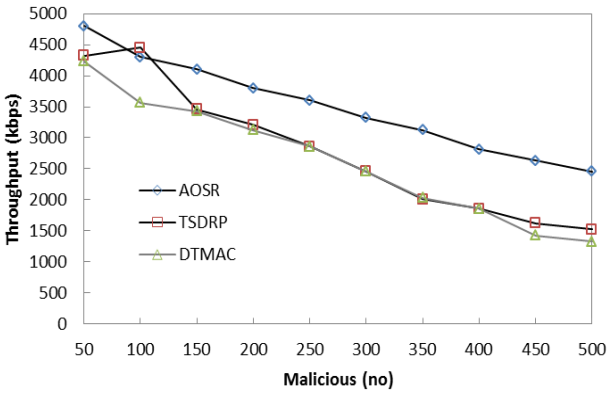

Figure 4.5: Effect of varying the number of nodes on the Normalized Rsouting Load

The outcome in figures 4.3, 4.4 and 4.5 speak to the ideal focuses which compares to the most elevated delivery ratio, least delay and the least routing load. It is discovered that for 60 nodes.

5.Conclusion

In any case, since it doesn't utilize source routing, it has a much lower start to finish delay for In request to investigate the exhibition of routing protocols practically speaking, such a situation based methodology is fundamental. It additionally recognizes the appropriate routing protocol for an ideal network size, the mobility of the nodes, the network thickness and a given traffic pattern. This section examines about the simulation-based way to deal with execution investigation of routing in MANETs. The section additionally examines some mobility models utilized for reproducing the development of nodes in an ad hoc network. A few other mobility models are being created which attempt to copy nature in which the nodes are sent. Such models are extremely helpful in increasing a more profound comprehension of the exhibition of routing protocols in practical organizations. The remainder of the part portrays a lot of situation-based examinations did to investigate the presentation of AOSR protocol in a front-line situation. The trials give an understanding into the working of the protocol in such a situation.

Reference

[1] Bakht, “Survey of routing protocols for mobile adhoc network”, International Journal of information and Communication Technology Research, vol. 1, no. 6, 2011.

[2] Chen and Heinzelman, “A survey of routing protocols that support QoS in mobile ad hoc networks”, Network, IEEE, vol. 21, no. 6, pp. 30–38, 2007.

[3] Abusalah, Khokhar and Guizani, “A survey of secure mobile ad hoc routing protocols”, Communications Surveys & Tutorials, IEEE, vol. 10, no. 4, pp. 78–93, 2008.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[4] Gupta, " Study the Effect of Mobility Model on Various Parameters by Varying Node Density in VANETs for TCP and CBR Applications", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 9, pp. 297–302, 2015.

[5] Pearlman and Samar, "The zone routing protocol (ZRP) for ad hoc networks", draft-ietfmanet-zone-zrp-04. txt, 2002.

[6] Park and Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks" ,in INFOCOM'97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution, Proceedings IEEE, vol. 3, pp. 1405–1413,1997.

[7] Murthy and Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks", Mobile Networks and Applications, vol. 1, no. 2, pp. 183–197, 1996.

[8] Stulman A, LahavJ, and Shmueli A. "Spraying Diffie-Hellman for secure key exchange in MANETs," In Security Protocols, XXI Springer Berlin Heidelberg, pp.202-212. 2012.

[9] Suresh, K.C., Prakash, S, Priya, AE & Kathirvel, A 2015, 'Primary path reservation using enhanced slot assignment in TDMA for session admission', The Scientific World Journal, Article: ID 405974.

[10] Yang Y. "A communication efficient group key distribution scheme for MANETs," In Network and System Security, Springer Berlin Heidelberg, 7645, pp.361-372, 2012.

[11] Chan A C. "Distributed private key generation for identity based cryptosystems in ad hoc networks", Wireless Communications Letters, IEEE, vol. 1, no.1, pp. 46-48, 2012.

[12] Palani1 U., Amuthavalli G., Chethan Prakash V. and Suresh K.C. "Energy-based Localization of IWSN in Biotechnology Industrial Applications" Res. J. Biotech ,Vol. (Special Issue II) August (2017)

[13] Li L C, and Liu R S. "Securing cluster-based ad hoc networks with distributed authorities," IEEE Transactions on Wireless Communications, vol. 9, no.10, pp. 3072-3081, 2010.

[14] Palani U, Suresh.K.C and Alamelu N, "Mobility Prediction In Mobile Ad Hoc Networks Using Eye Of Coverage Approach", Journal Of Cluster Computing, 2018

[15] Yang Y. "Broadcast encryption based non-interactive key distribution in MANETs," Journal of Computer and System Sciences, vol. 80, no.3, pp. 533-545, 2014.

[16] ZHANG Y, and QIAN H F. "An efficient identity-based secret key management scheme for MANETs," The Journal of China Universities of Posts and Telecommunications, vol. 19, pp.127-136, 2012.

[17] Suresh K.C., Haripriya K. and Kruthika S.R."Cooperative Multipath Admission Control Protocol: A Load Balanced Multipath Admission Policy", Research Journal of Biotechnology, Vol. (Special Issue II), August (2017)

[18] Hyun-oh Shin, Doo-yeol yoo, Joo-Ha Lee, Seung-Hoon Lee, Young-Soo Yoon. Optimized mix design for 180Mpa ultra-high-strength concrete.(2019).

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731