Original Article

SECURED MULTI AGENT RAPID TRUSTY ADHOC ON-DEMAND DISTANCE VECTOR (SMART-AODV) ROUTING PROTOCOL FOR SERVICE DISCOVERY PROCESS IN MANET

S. John Grasias[1], Dr. B. Sureshkumar[2]

[1] Research Scholar, Department of Computer Science, AJK College of Arts & Science, Navakkarai (po), Coimbatore, India.
[2] Assistant Professor, Department of Computer Science, AJK College of Arts & Science, Navakkarai (po), Coimbatore, India.

DOI: 10.47750/pnr.2022.13.S08.391

Abstract

Mobile Adhoc Network (MANET) is a network of a number of mobile routers and related hosts, coordinated in a random fashion through wireless links. Service Discovery is one of the main issues in MANET. It is characterized as the process of facilitating service providers to publicize their services in a dynamic manner and to permit consumers to find and access those services in a proficient and adaptable way. A service discovery protocol is a protocol that permits automatic detection of devices and services presented by these devices. Service discovery in mobile impromptu networks is challenging a direct result of the shortfall of any central coordinator in the network. Here agents travel through the network, gathering the dynamically changing service information. Be that as it may, dependability and accessibility issues are should have been tended to while planning mobile agent based (service discovery) protocols before it very well may be conveyed for an expansive scope of commercial applications in MANET. This paper proposes Secured Multi Agent Rapid Trusty Adhoc On-Demand Distance Vector (SMART-AODV) Routing Protocol for Service Discovery Process in MANET. The proposed Secured Multi Agent Rapid Trusty Adhoc On-Demand Distance Vector (SMART-AODV) Routing Protocol gives a complete solution as far as improving power increase, bandwidth conservation, and secures path selection.

Keywords: MANET, Service Discovery, Networks, Mobile, Protocol.

Introduction

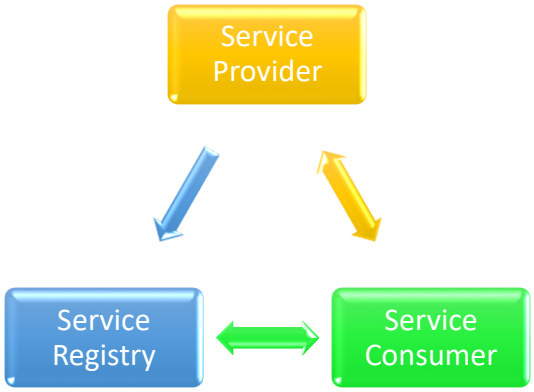
Mobile Ad hoc Networks are framework less networks that are outlined among a number of mobile nodes. Because of the dynamic idea of these sorts of networks, algorithms that were intended for customary networks (for example routing, transport protocols, security and QoS) don't show good execution for MANET. As a result dynamic research work is proceeding to propose new algorithms and protocols for MANET. Service Discovery in MANET is one such issue that has acquired considerable consideration during late years. A service is any unmistakable or impalpable asset that one can conjure to acquire some utility. Service Discovery can be characterized as the most common way of discovering a few service for the benefit of its client in light of the inclinations (for example QoS) specified by the client and limitations (for example cost) specified by the supplier.

Service Discovery can find a network naturally making it with the goal that there is no requirement for a long design set up process. Service discovery works by gadgets interfacing through a typical language on the network permitting gadgets or services to associate with no manual intercession. (i.e, Kubernetes service discovery, AWS

service discovery) There are two kinds of service discovery: Server-side and Client-side. Server-side service discovery licenses client's applications to find administrations through a switch or a load balancer. Client-side service discovery permits clients applications to track down services by glancing through or questioning a service registry, in which service occasions and endpoints are all inside the service registry.

A lot of research is being completed to settle different issues of MANET. These issues incorporate Routing, MAC Layer Issues, Power Management, and Transport convention, Quality of Service, Billing, Addressing, Service Discovery, Data Management and Security and so forth One of the main inquiries in MANET is the discovery of services accessible around the vicinity of any node. A service can be any hardware, software or whatever other entity that a client may be intrigued to use and Service Discovery is the most common way of discovering the services in view of client inclinations. An efficient and scalable way to deal with service discovery can prompt the advancement an enormous number of expected applications. For instance, in a vehicular specially appointed network, vehicles may be keen on realizing the services given by a close by fuel station. Additionally, in a war zone officers may be keen on sharing what is happening about the entire war zone.

Figure 4.1 Service Discovery



Service Discovery in MANET gives a number of helpful advantages to the end client. For instance: in the event that you are going on a vehicle and accepting an Ad hoc network is framed between vehicles around you. You can use a number of location based services while meandering along the street. This incorporates street security services (for example climate cautioning, mishap data, backup way to go help) or non security services (for example M-Banking, finding an eatery/stopping/fuel station). In the majority of these cases, a number of service discovery requests are given all the while. We can call such concurrent requests as having a place with one service meeting. Normally, the service discovery requests that are given in one meeting are connected. For instance, assuming the client goal is shopping, his requests will be to discover the shopping centers around it, the shopping things accessible at the shopping center, the expense of individual things and so forth Our inspiration is that assuming we can some way or another discover connection among the services of one meeting, we can foresee future discovery requests in view of current service discovery demand. In our research, we have utilized the Association Rules mining calculation to accomplish this goal. Utilizing the relationship among the services and piggybacking future service demand replies alongside current service requests, we have demonstrated huge increase in execution.

Literature Survey

1. Konark et.al proposed service discovery and delivery protocol specifically for ad-hoc, peer-to-peer networks, and designated towards gadget independent services overall and m-commerce situated software services specifically. It has two significant viewpoints service discovery and service conveyance. For discovery, Konark utilizes a totally disseminated, distributed component that gives every gadget the capacity to promote and discover

services in the network. The methodology towards service depiction is XML based. It incorporates a depiction format that permits services to be portrayed in a human and software reasonable structures. Konark gives a framework to interfacing segregated services presented by proximal pervasive devices over a wireless medium.

2. Allia et.al proposed peer-to-peer caching based and policy-driven agent service discovery framework to facilitate cross-stage service discovery in impromptu conditions for mobile electronic commerce applications. This approach eliminates the issues related with structured compound arrangement of specialist networks in mobile commerce climate and accomplishes serious level of flexibility in adapting itself to the progressions of the impromptu climate. This framework thinks about gadget capacities and restrictions, client inclinations in regards to use of the devices, application particulars as for mobile commerce and adapts accordingly.

3. Tamer Rafael et al. proposed a standing instrument, which is sent inescapable in every one of the nodes present in an impromptu network. In this system, the node utilizes two substances in particular standing file and a standing table. Notoriety list of a node used in this component might be characterized as a monotonically expanding esteem registered concerning the fruitful conveyance of bundles to its neighbors. The standing table thus stores the refreshed standing list at every single time meeting of correspondence. The creators have additionally proposed this instrument in view of three heuristic methodologies to be specific Hops from source, twofold decrement/single augmentation proportion and arbitrary early probation.

4. U. C. Kozat and L. Tassiulas et.al proposed solution is a conveyed service discovery design that depends on a virtual backbone for finding and enlisting accessible services. The proposal comprises of two independent components. The primary part is arrangement of a virtual backbone and the subsequent one is dissemination of service registrations, requests and answers. In their network model, apportioning isn't considered the purpose of consensus; since each parcel might be treated as an independent network. The proposal upholds registry engineering and for this reason, the network level arrangement is developed in two sections. Initial one is the BBM (Backbone Management) stage where a subset of generally stable network nodes are chosen as the ruling set and adapting this ruling set to the geography changes by adding or eliminating nodes into/from the set. BBM utilizes just 1-jump nearby transmission control message which are classified "hello beacons" to from backbone set, make virtual connection between backbone nodes and keep up with the backbone. At the point when the BBM stage is effectively finished, the network will have network structured virtual backbone which is named as "black nodes".

5. Wei Yan et.al proposed have proposed a new resource discovery framework that leverages the properties of appropriated content-based publish or subscribe frameworks. Static, dynamic and ceaseless are the three discovery models upheld by their asset discovery framework. Resources with fixed attributes are discovered in static model, if there should arise an occurrence of dynamic discovery model attributes of resources can be refreshed, and warnings to the recently enlisted resources are sent utilizing the nonstop model. Every one of the three models can exist together in one framework and supplement each other. What's more, a comparability based enhancement calculation is introduced that uses publish/subscribe covering strategies to reuse the discovery results among various simultaneous discovery requests.

Proposed Methodology

Wireless impromptu on-demand distance vector routing protocol is receptive directing protocol with route discovery and route upkeep. The chose AODV as a base due to its reactive nature and furthermore it makes less bundles upward when contrasted with other routing protocols. To accomplish service discovery in AODV routing process, every node need to keep a service table to record the service information. We have additionally addressed the issue of trust based routing schemes in a MANET, which generally consider most trustworthy nodes in a route. Because of this conduct of trust based routing, the trustworthy nodes of the network are overburdened in routing only and they can't play out their normal task efficiently. To stay away from this issue we, attempt to look through multiple trustworthy routes between similar source and destination and use them all the while to send data bundle. So this stage proposed Secured Multi Agent Rapid Trusty Adhoc On-Demand Distance Vector (SMART-AODV) Routing Protocol for Service Discovery Process in MANET.

In the algorithm, the agents convey the RREQ bundles with them and track down the route between the source and the destination. Whenever the agent compasses to the neighboring node, the agent will check for the destination address. On the off chance that the address is found in the routing table of the node, it does the further processing in any case again the agent move to the following neighbor node. The process continues till the agent observes the destination address. The benefit of utilizing the mobile agent is that the agent chips away at the disconnected operation. They only require the bandwidth at the time of roaming in the network. What's more the power of the node is additionally optimized.

Figure 4.2 Transferring the MA to the neighboring node

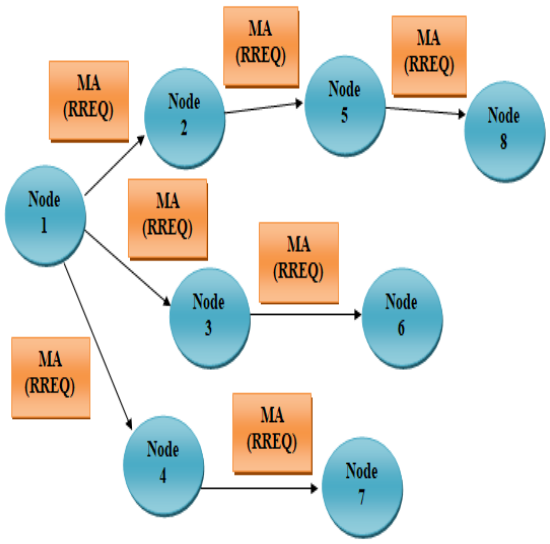


Figure 4.2 is depicting the transferring of mobile agents by the source node in the network.

The proposed Secured Multi Agent Rapid Trusty Adhoc On-Demand Distance Vector (SMART-AODV) Routing Protocol can be utilized in mobile impromptu network for identifying and staying away from rowdiness of the nodes. The source node is the initiator of the route discovery process in this routing plan. It makes a mobile agent (MA) and the mobile agents will convey the RREQ bundle, and broadcast it to every one of its neighbors. The neighbor nodes further transmission mobile agent (MA) with RREQ to their neighbors until mobile agent (MA) comes to at destination node. In the unlikely event that there is a path between sender to receiver in routing table, value of the receiver sequence number in the section containing the path passage and the receiver sequence number in the parcel RREQ will be analyzed. If, despite everything that the receiver sequence number in RREQ parcel is more prominent than the sequence number in the routing table, it won't use path of the guiding table to pay all due respects to the source node. Furthermore the mobile agent will forward ahead with the RREQ parcel to the following node and the number of hops will be expanded by 1.

At destination node for each got RREQ, a RREP is made and else, MA will move back with RREP pack taken from the node to avow the receipt of RREQ parcel. Along with hop count and TTL. Time to live (TTL) lifetime of data in a network, at that point, it sent back to the source node on a similar path from where the RREQ came. In the unlikely event that there is no sender to the receiver in the routing table, the mobile agent will push ahead to the following node with RREQ parcel. The agent will consequently set up an opposite way to a sender. The mobile agent will keep the track with the hop count and TTL and the largest sequence number. Simultaneously the destination node will work out the trust value of the following hop neighbor and add that value into the RREP. Each halfway node which receives the RREP further calculates the trust value of their next hop neighbor and adds that trust value into RREP prior to forwarding it.

This process is rehashed on each middle node until RREP comes to at the source node. The source node receives multiple mobile agents will return with RREP parcel with a trust value appended to each, the mobile agent having a largest sequence number and minimum hop count will be picked and the path is refreshed in the routing table.

The source node calculates normal of all trust values got with RREPs and all the while utilizes the RREPs with trust value more than the normal trust value for data transmission.

Trust Calculation

Trust calculation is a function which receives all noticed parameters of a node and returns a determined trust value of the node. This function totals all parameters as a one trust value. The Trust based routing is the extension of AODV routing, which utilizes the trust calculation module to take routing decisions while shaping route from source to destination.

For computing the trust value, following method is utilized. Assuming the node b whose trust value is needed, on the off chance that the section for node b is send off in trust table of node a. Then, at that point, it refers the trust table on a node and gain perceived and saved value for given node b. Here we appoint a few attributes for neighbor node b. i.e,

$$pac_{rec_b} = No\ of\ packets\ recognized\ for\ a\ neighbour\ node\ b$$

$$pac_{del_b} = No\ of\ packets\ profitably\ delivered\ at\ neighbour\ node\ b$$

$$pac_{ppd_b} = No\ of\ packets\ postponed\ \ at\ neighbour\ node\ b$$

$$pac_{brk_b} = No\ of\ link\ breaks\ due\ to\ node\ b$$

Then, calculate x, y, z

$$x = pac_{rec_b} - pac_{del_b}$$

$$y = pac_{ppd_b}$$

$$z = pac_{brk_b}$$

After that, compute theD_1, D_2, and D_3 at a node using observed values.

$$D_1 = \left(\frac{x}{x+y+z}\right)$$

$$D_2 = \left(\frac{y}{x+y+z}\right)$$

$$D_3 = \left(\frac{z}{x+y+z}\right)$$

$$t\_v_{a,b} = -D_1 * (x) - D_2 * (y) - D_3(z)$$

if the entry for node b is not in trust table of node a then fix

$$t\_v_{a,b} = threshold\ value$$

Trust value of a node b at node a is $t\_v_{a,b}$.

The underneath algorithm depicts multiple paths from source node to destination node with the trust value of every path on source nodes routing table.

ALGORITHM 1: Secured Multi Agent Rapid Trusty Adhoc On-Demand Distance Vector (SMART-AODV) Routing Protocol

Initialize *Source Node = SN, Destination Node = DN, Trust Value = t_v, Largest sequence number = LSN;*

S1: Start the process.

S2: At SN creates the MA with RREQ packet with DN address.

S3: SN broadcasts MA with RREQ to all its neighbours

S4: ***For*** *each neighbour node of SN*

S5: ***While*** *(MA with RREQ not reached to DN)*

S6: *RREQ is further broadcasted*

S7: ***end loop***

S8: *MA with RREP is created at DN with t_v=0, TTL=0, hop_count=0,LSN=0;*

S9: *next_node=DN*

S10: ***While****(next_node is not SN)*

S11: *next_node=next hop neighbour*

S12: *search for entry of next_node in trust table*

S13: *Calculate (t_v, TTL & LSN)of next_node*

S14: *Update RREP with t_v+=calculated t_v*

hop_count++;

S15: *Unicast MA with RREP to next_node*

S16: ***End loop***

S17: ***if*** *(next_node is SN)*

S18: *Route is stored in the routing table of SN*

S19: ***End if***

S20: ***End for***

Step 21: threshold_value= largest sequence no & minimum hop count & average of trust value of all routes.

Step 22: ***For*** *each route*

Step 23: ***if*** *(t_v of route < threshold_value)*

Step 24: *remove the route from the routing table*

Step 25: ***end if***

Step 26: ***end for***

Step 27: ***while*** *(source has a data packet to send)*

Step 28: ***for*** *j=1 to N: number of routes from SN to DN in the routing table*

Step 29: *use route j to send data packet*

Step 30: ***end for***

Step 31: ***end while***

Step 32: Stop the process.

Experimental Result

Service Discovery Time:

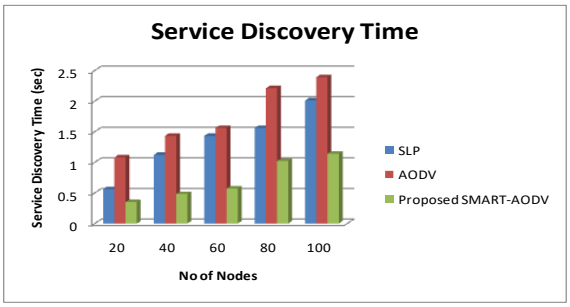
Response time which is additionally considered as service discovery time in our proposed plot is displayed in Fig. 4.3, which portrays that the time our mechanism takes to discover services inside the network step by step increments as we increment the number of hubs in the network. It very well may be determined that density of the network influences the service discovery time.

Table 4.1 Comparison table of Service Discovery Time

Number of Nodes	SLP	AODV	Proposed SMART-AODV
20	0.56	1.08	0.35
40	1.12	1.43	0.48
60	1.43	1.56	0.57
80	1.56	2.21	1.02
100	2.01	2.39	1.14

The comparison table of Service Discovery Time describes the different values of existing (SLP, AODV) and proposed SMART-AODV. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 0.56 to 2.01 and 1.08 to 2.39. The proposed SMART-AODV values start from 0.35 to 1.14. The proposed SMART-AODV gives the best result.

Figure 4.3 Comparison table of Service Discovery Time



The figure data Service Discovery Time describes the different values of existing (SLP, AODV) and proposed SMART-AODV method. While comparing the existing and the proposed SMART-AODV method values are higher than the existing method No of Nodes in x axis and Service Discovery Time in Y axis. The existing values start from 0.56 to 2.01 and 1.08 to 2.39. The proposed SMART-AODV values start from 0.35 to 1.14. The proposed SMART-AODV gives the best result.

Packet delivery ratio

The packet delivery ratio can be gotten from the complete number of data packets showed up at objections partitioned by the all out data packets sent from sources. At the end of the day Packet delivery ratio is the ratio of number of packets got at the objective to the number of packets sent from the source. The exhibition is better when packet delivery ratio is high.

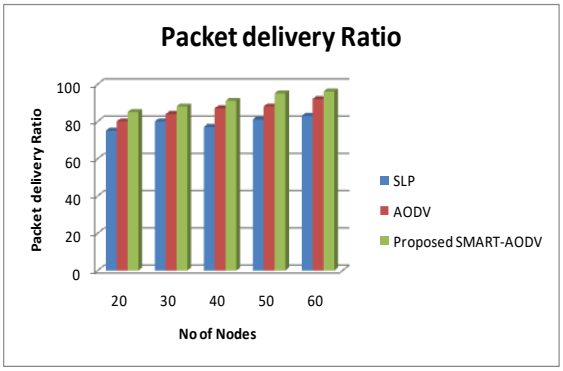
$$Packet\ Delivery\ Ratio\ = \frac{\sum(Total\ packets\ recived\ by\ all\ DN)}{\sum(Total\ packets\ send\ by\ all\ SN)}$$

Table 4.2 Comparison table of Packet delivery ratio

Number of Nodes	SLP	AODV	Proposed SMART-AODV
20	75	80	85
30	80	84	88
40	77	87	91
50	81	88	95
60	83	92	96

The comparison table of Packet delivery ratio describes the different values of existing (SLP, AODV) and proposed SMART-AODV. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 75 to 83 and 80 to 92. The proposed SMART-AODV values start from 85 to 96. The proposed SMART-AODV gives the best result.

Figure 4.4 Comparison table of Packet delivery ratio



The figure data Packet delivery ratio describes the different values of existing (SLP, AODV) and proposed SMART-AODV method. While comparing the existing and the proposed SMART-AODV method values are higher than the existing method No of Nodes in x axis and Packet delivery ratio Time in Y axis. The existing values start from 75 to 83 and 80 to 92. The proposed SMART-AODV values start from 85 to 96. The proposed SMART-AODV gives the best result.

Throughput

Throughput is characterized as the ratio of the total data arriving at a collector from the shipper. The time it takes for the recipient to when it's all said and done the last message is called throughput. Throughput is conveyed as bytes or bits per sec (byte/sec or bit/sec). A few factors influence the throughput as; assuming that there are numerous geography changes in the network, temperamental communication between nodes, restricted bandwidth accessible, and restricted energy. High throughput is a flat out decision in each network.

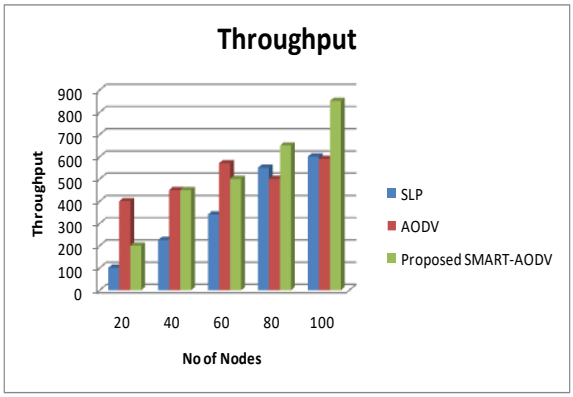
$$Throughput = \frac{File\ size}{Transmission\ Time}$$

Table 4.3 Comparison table of Throughput

Number of Nodes	SLP	AODV	Proposed SMART-AODV
20	100	400	200
40	225	450	450
60	340	570	500
80	550	500	650
100	600	590	850

The comparison table of Throughput describes the different values of existing (SLP, AODV) and proposed SMART-AODV. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 100 to 600 and 400 to 590. The proposed SMART-AODV values start from 200 to 850. The proposed SMART-AODV gives the best result.

Figure 4.5 Comparison table of Throughput



The figure data Throughput describes the different values of existing (SLP, AODV) and proposed SMART-AODV method. While comparing the existing and the proposed SMART-AODV method values are higher than the existing method No of Nodes in x axis and Throughput in Y axis. The existing values start from 100 to 600 and 400 to 590. The proposed SMART-AODV values start from 200 to 850. The proposed SMART-AODV gives the best result.

Total energy Consumption

Total energy consumption for every one of the simulations and isolated by the total number of effectively gotten bytes. The underneath table gives the normal energy consumption in various situations. This table is acquired by averaging the energy consumption for each routing protocol, for every transmission rate and the quantity of nodes.

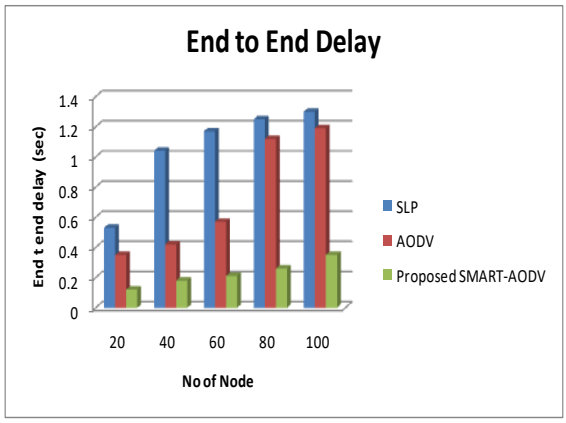
$$E_{N/M} = 1_{n>0}\left(1_{M=N}E_{T_{ack}} + 1_{M\neq N}E_{R_{ack}}\right) + 1_{m>0}\left(1_{M=N}E_{T_{pck}} + 1_{M\neq N}E_{R_{pck}}\right)$$

Table 4.4 Comparison table of Total energy Consumption

Number of Nodes	SLP	AODV	Proposed SMART-AODV
20	850	300	200
40	900	550	355
60	1200	680	480
80	1100	925	590
100	1400	1100	760

The comparison table of Total energy Consumption describes the different values of existing (SLP, AODV) and proposed SMART-AODV. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 850 to 1400 and 300 to 1100. The proposed SMART-AODV values start from 200 to 760. The proposed SMART-AODV gives the best result.

Figure 4.6 Comparison table of Total energy Consumption



The figure data Total energy Consumption describes the different values of existing (SLP, AODV) and proposed SMART-AODV method. While comparing the existing and the proposed SMART-AODV method values are

higher than the existing method No of Nodes in x axis and Total energy Consumption in Y axis. The existing values start from 850 to 1400 and 300 to 1100. The proposed SMART-AODV values start from 200 to 760. The proposed SMART-AODV gives the best result.

End to end delay

End to end delay is determined as the ratio of each bundle sent from the source node to the quantity of data parcels got at the objective node. This metric is highly essential to assess the Jellyfish attack sway on MANET. It is determined utilizing the accompanying formulae:

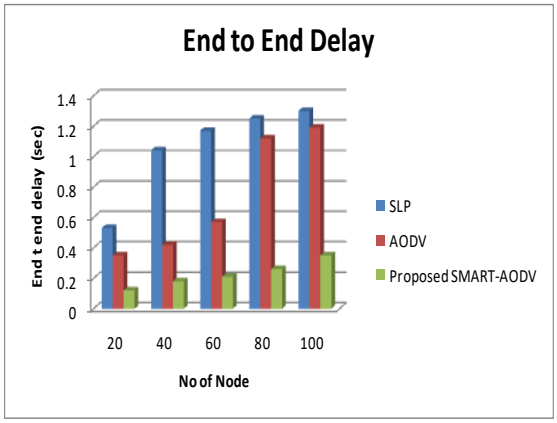
$$End\ to\ end\ delay\ \Delta = \frac{\sum_{i=1}^{N_{rcd}} \Delta_i}{N_{rcd}}$$

Table 4.5 Comparison table of End to end delay

Number of Nodes	SLP	AODV	Proposed SMART-AODV
20	0.53	0.35	0.12
40	1.04	0.42	0.18
60	1.17	0.57	0.21
80	1.25	1.12	0.26
100	1.30	1.19	0.35

The comparison table of End to end delay describes the different values of existing (SLP, AODV) and proposed SMART-AODV. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 0.53 to 1.30 and 0.05 to 1.19. The proposed SMART-AODV values start from 0.12 to 0.35. The proposed SMART-AODV gives the best result.

Figure 4.7 Comparison table of End to end delay



The figure data End to end delay describes the different values of existing (SLP, AODV) and proposed SMART-AODV method. While comparing the existing and the proposed SMAVM method values are higher than the existing method No of Nodes in x axis and End to end delay in Y axis. The existing values start from 0.53 to 1.30

and 0.05 to 1.19. The proposed SMART-AODV values start from 0.12 to 0.35. The proposed SMART-AODV gives the best result.

Conclusion

The vision of pervasive computing as well as surrounding insight requires empowering ubiquitous computing and networking with the goal that mobile users can seamlessly gain admittance to digital services anywhere, anytime. MANETs are one empowering influence of such a vision, giving networking abilities to mobile devices without requiring any infrastructure. Be that as it may, the particulars of MANETs like possibly exceptionally dynamic topology and networking of heterogeneous wireless nodes whose energy should be put something aside for enhanced autonomy; require unique care in the treatment of distributed service provisioning. In this phase, proposes Secured Multi Agent Rapid Trusty Adhoc On-Demand Distance Vector (SMART-AODV) Routing Protocol for Service Discovery Process in MANET. The results of this proposed trust based mechanism for service discovery makes it obvious that it provides better performance in terms of Packet Delivery Ratio, Total overhead, Control overhead and Throughput.

References

1. N. Islam, "A Secure Service Discovery Scheme for Mobile ad hoc Network using Artificial Deep Neural Network," 2019 International Conference on Frontiers of Information Technology (FIT), 2019, pp. 133-1335, doi: 10.1109/FIT47737.2019.00034.
2. A. Golzadeh and M. Niamanesh, "DSDST - A Distributed Service Discovery Approach with Service Type for Mobile Ad Hoc Networks," 2011 Second International Conference on Networking and Distributed Computing, 2011, pp. 267-271, doi: 10.1109/ICNDC.2011.61.
3. H. Tsai, T. Chen and C. Chu, "Service Discovery in Mobile Ad Hoc Networks Based on Grid," in IEEE Transactions on Vehicular Technology, vol. 58, no. 3, pp. 1528-1545, March 2009, doi: 10.1109/TVT.2008.928003.
4. V. Raychoudhury, J. Cao, W. Wu and C. Chen, "Service Handoff for Reliable and Continuous Service Access in MANET," 2011 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing, 2011, pp. 172-179, doi: 10.1109/PDP.2011.30.
5. R. Neogy, C. Chowdhury and S. Neogy, "A reliable service discovery protocol using mobile agents in MANET," 2012 Proceedings Annual Reliability and Maintainability Symposium, 2012, pp. 1-7, doi: 10.1109/RAMS.2012.6175451.
6. A. Nedos, K. Singh, R. Cunningham and S. Clarke, "Probabilistic Discovery of Semantically Diverse Content in MANETs," in IEEE Transactions on Mobile Computing, vol. 8, no. 4, pp. 544-557, April 2009, doi: 10.1109/TMC.2008.133.
7. K. Venkatesh, N. Nithiyanandam and Sivaneshkumara, "ANFIS based QoS-aware Routing Protocol for Video Streaming in MANETS," 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2019, pp. 1-6, doi: 10.1109/INCOS45849.2019.8951346.
8. M. Hormati, F. Belqasmi, R. Glitho and F. Khendek, "A DNS protocol - based Service Discovery architecture for disaster response systems," 2013 IEEE Symposium on Computers and Communications (ISCC), 2013, pp. 000366-000371, doi: 10.1109/ISCC.2013.6754974.
9. Aakanksha and P. Bedi, "Mobile process groups based device/service discovery and interoperability in MANets," 2012 12th International Conference on Intelligent Systems Design and Applications (ISDA), 2012, pp. 466-471, doi: 10.1109/ISDA.2012.6416583.
10. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and D. Gaiti, "Denial of Service (DoS) attacks detection in MANETs through statistical models," 2014 Global Information Infrastructure and Networking Symposium (GIIS), 2014, pp. 1-3, doi: 10.1109/GIIS.2014.6934261.
11. C. Lal, V. Laxmi and M. S. Gaur, "QoS-aware routing for transmission of H.264/SVC encoded video traffic over MANETs," 2013 19th Asia-Pacific Conference on Communications (APCC), 2013, pp. 104-109, doi: 10.1109/APCC.2013.6765924.
12. J. Kniess, L. Arantes, P. Sens and C. V. N. Albuquerque, "Saving Resources in Discovery Protocol on Delay-Sensitive Rescue Mobile Networks," 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), 2017, pp. 538-545, doi: 10.1109/AINA.2017.81.
13. I. Ullah, G. Abbas and Z. H. Abbas, "Energy-aware congestion-less dynamic source routing for MANETs," 2017 International Multi-topic Conference (INMIC), 2017, pp. 1-6, doi: 10.1109/INMIC.2017.8289471.

14. M. al Mojamed and M. Kolberg, "OLSR Optimisation for Lightweight MANET Internet Integration," 2019 12th International Conference on Information & Communication Technology and System (ICTS), 2019, pp. 141-145, doi: 10.1109/ICTS.2019.8850981.

15. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and D. Gaiti, "Denial of service (DoS) attacks detection in MANETs using Bayesian classifiers," 2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), 2014, pp. 7-12, doi: 10.1109/SCVT.2014.7046699.