International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5884-5893

Power Optimized Secure AODV Routing Protocol Based on Mobile Agents

Bindiya Bhatia
Department of Computer Science & Engineering, Manav Rachna International University,
Sec 43 Aravali Hills Delhi Surajkund Road, Faridabad, India

Orcid Id: 0000-0003-0372-9238

M.K. Soni
Department of Electronics & Communication Engineering
Manav Rachna International University, Sec 43 Aravali Hills Delhi Surajkund Road
Faridabad, India 121004

Parul Tomar
Department of Computer Engineering, YMCA University of Science & Technology
Mathura Road, Faridabad, Pin code- 121006, India
Orcid Id: 0000-0002-3917-3369

Abstract

In Mobile ad-hoc networks (MANET), route optimization and power conservation are the critical issues and a requirement of an efficient routing protocol is always there to make the MANET reliable and tackle these issues. In recent years, researchers have proposed various routing algorithms to save the resources of the node such as energy, bandwidth, and computing power etc. Power Conservation is the enormous issue to be handled because the mobile devices work on battery which has limited processing power. Ad-Hoc on Demand Distance Vector (AODV) is the most common and a good performer protocol in MANET. In order to make the AODV routing protocol power optimized and secure, the protocol is modified and an extended algorithm is proposed based on mobile agents. The mobile agents are autonomous and intelligent small programs which can roam around the network. They can be used by the protocol to share the routing information. Due to its disconnected operation, the battery power of a node can be optimized thus making the algorithm power efficient. Also, the algorithm provides a secure optimal path by comparing multiple paths for the destination. The proposed algorithm is compared with the conventional AODV on the basis of the performance metrics: Packet delivery ratio, energy consumed and throughput.

Keywords: Mobile ad-hoc networks, mobile agents, routing, AODV, power efficient

INTRODUCTION

With the advancement of wireless technologies such as Bluetooth or 802.11 standards, the mobile ad-hoc network is gaining attention as a next leading edge for wireless communication in various disciplines such as military, vehicle, disaster etc. Mobile ad-hoc networks (MANET) are self-configuring and self-forming infrastructure less networks [1]. The network is formed without any centralized entity. The seamless communication is provided by mobile ad-hoc networks because the nodes themselves create the networks dynamically. There is no pre arrangement with respect to a particular part that every node ought to accept. In the light of the above mentioned network situation, every node takes its decision freely, without utilizing any pre-existing infrastructure. For e.g. two PCs can communicate with each other if they are within the transmission range of each other through wireless adapter cards. Thus, MANET provides significant advantages over wired technologies such as less infrastructure cost, fault-tolerance, ease in forming the network and easy deployment. The mobile devices with in the transmission range can form the network and communicate with each other anywhere, anytime. Due to the absence of supporting infrastructure, the nodes send the packets to the neighboring nodes through peer to peer communication. The intermediate network nodes can act as a router in the network and relay the packets hop by hop. This multi-hoping reduces the requirement of any centralized structure. These intermediate nodes participate in route discovery and route maintenance. Even, not exclusively can mobile devices converse with each other, additionally get Internet benefits through an Internet gateway, amplifying both network and Internet amenity to the zones where there is no infrastructure.

In order to make this possible, there are several routing protocols across the networks. The protocols diverge in techniques employed to determine routes and maintaining the routes and stratified as reactive (Ad-Hoc On Demand Distance Vector (AODV) routing, Dynamic Source Routing

(DSR), Temporally Ordered Routing Algorithm (TORA), Associativity Based Routing (ABR) etc.), proactive (Destination Sequence Distance Vector(DSDV), Optimized Link State Routing Protocol(OLSR), Wireless Routing Protocol (WRP), Global State Routing(GSR) etc.) and hybrid(Zone Routing Protocol(ZRP)) protocols [2,3,4,5,6,7,8]. But these routing protocols in MANET come with a cost. The routing protocol requires memory, computational resources and battery power for establishing the routes between the nodes. Even as the network grows, the requirement increases to maintain the routing information and hence results in to congestion overhead and more battery power consumption. Power Conservation is the enormous issue to be handled because the mobile devices work on a battery which has limited processing power. Every node has a role of an end system as well as a router at the same moment, which requires more power to send the packets. Also, there is a need to lower the control overheads. Security is another issue that needs to tackle because MANET is more susceptible to threats than any fixed wired network. MANET relies on individual security solution on each node as a centralized security solution is not easy to put into operation. The interaction between mobile devices in MANET is exigent because of the frequent link changes and limited bandwidth. The mobile nodes interact over comparatively bandwidth constrained wireless links. So, it is important to design a protocol that is bandwidth efficient. Besides this, due to a dynamic topology change, finding the optimal route is also a challenging task.

In sight of these challenges, a novel algorithm is proposed which is based on the application of mobile agents in AODV Routing Protocol in order to optimize the power and provide optimized secure routing. The mobile agents don't require bandwidth at the time of processing and thus making the algorithm bandwidth and power optimized. Different and advantageous communication manner of mobile agents makes it more suitable in MANET. Results in the subsequent section shows that applying mobile agents in AODV makes it more power optimized, secure and bandwidth efficient.

The paper is dividing into seven sections. The next section of the paper discusses mobile agents. Further, section III illustrates the normal working of AODV and section IV is throwing light on the advancements in AODV. Section V is putting forward the proposed modified AODV routing algorithm based on mobile agent. Section VI shows the simulation and results of the proposed intended algorithm and the comparison between the traditional AODV and the proposed algorithm in terms of the performance metrics: PDR, energy, throughput. Section VII concludes the paper.

MOBILE AGENTS PARADIGM

Mobile Agents are a compelling worldview for distributed application, and are especially appealing in dynamic network conditions [9, 10]. One of the qualities of mobile agent paradigm is the likelihood of moving the complex functionality to the device where a large sum of data is to be exercised.

Mobile Agents can be contemplated as an incremental development of the prior thought of "process migration". Mobile agents are self-governing programs that can move from node to node, interacting with the devices and the other agents [11, 12]. The running application's state can be saved and carried to the new host, permitting the application to proceed with execution from where it left off before relocation. Mobile Agent innovation offers a few impending advantages over regular client-server processing that could help enhance the standard distributed framework, which is typically stand on the notable remote procedure call (RPC) or remote method Invocation (RMI). The client-server architecture tightly binds the client and the server. It expects that there is no constraint on the bandwidth accessibility between the nodes and in addition the availability and reliability of the nodes. Mobile agent's inborn features as autonomy and disconnected operation give the advantage over this situation. Mobile Agent's mobility allows an agent to work on the device where the data resides. And the disconnected operation optimizes the requirement of bandwidth to complete the task. The connection can be disconnected between devices when the mobile agent reaches to do the processing on the device. As soon as the processing is completed the device can reconnect to the network and the agent can carry back the results. The mobile agent can filter the information at the server side and return back to the client only the pertinent information. Thus the client gets the minimized information and need not to do any filtration [13].

Tablets, Personal Digital Assistant (PDA) and home and business PCs are associated with the network over a modem Connection. These gadgets frequently have low-data transfer capacity and frequently change their network address with every reconnection. Mobile Agents straightforwardly address these issues. A mobile agent can roam around the network and access the needed resources. It moves directly to the tablets or laptops instead of exchanging multiple request and responses over the low-bandwidth connection for data access. Figure 1 is showing the working of mobile agents. Since it is not in a direct interminable contact with the devices, the device is not influenced if the connection is lost suddenly. The agent can continue its task on the remote device, even the user shuts down or disconnected. Whenever the user reconnects, the agent returns back with the results of the processing. Mobile Agents are easy to deploy and test because they hide the communication channel detail except at the time of traveling [14, 15]. Mobile Agents move around the network autonomously and select its destination itself. The mobile agent paradigm has moved the user from typical client-server model to more adaptable peer to peer model in which a system can act as a server or client according to the present need [16, 17, 18]. Effortlessly moving the task to appropriate network location tends to the scalability of the applications [19, 20, 21].

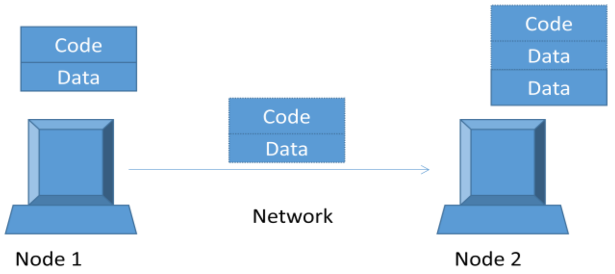

Figure 1: Concept of Mobile Agent

CONVENTIONAL AODV

AODV is a reactive routing algorithm which enables a dynamic, self-initiating multi-hop routing whenever a node urges to send data to a particular node [22]. AODV is able to do unicast and multicast routing. There are 4 types of message formats in AODV for finding a path:

Route Request Message (RREQ): Whenever a node wants to send the data to a particular node, the RREQ packet is broadcasted to the network.

Route Reply Message (RREP): Whenever the node has a route to the destination node, it replies back to the source node.

Route Error Message (RERR): Whenever a link failure is there, a route error is sent to the nodes of both the sides to give information about the link failure.

Route Reply Acknowledgment Message Format (RREP-ACK): In response to RREP message an acknowledgment is sent as a route reply message.

In AODV, a sequence number is maintained by each destination node. The entry in the routing table contains the destination sequence number signifying the time of the route creation at the destination node. The RREQ message contains the initiator's sequence number and the destination node's sequence number. Before the initiator issues a RREQ message it increments its own sequence number. After getting the RREQ message, the node updates the path in its routing table with the initiator's sequence number if this number is greatest among all the available routes. If a node is getting multiple RREQ messages and the initiator's sequence number is same then the node takes the path to the initiator having lower hop count. To check whether the route is up to date or not, we make sure that this node's destination sequence number is greater than the maximum destination sequence number of all the nodes through which RREQ message is routed. When the destination node responds with the RREP, it updates its own sequence number with the greatest of its recent sequence number and destination sequence number which is included in RREQ packet.

The AODV works in two phases: one is route discovery, in which the path is located between the source and the destination and the other is route monitoring, in which the path is monitored for link breakage. The two phases are explained below in detail:

Route Discovery: When a node wants to send a packet to a particular node then route discovery process initiated. The node broadcasts the RREQ message to all the neighboring nodes. The destination's last known sequence number is attached with RREQ. If the sequence number is not known then an unknown sequence number flag is set. After receiving the RREQ message, the node replies with RREP message if the node itself is a destination or it has a path to the destination node. If a node is itself a destination, it will increment its own sequence number by one in the RREP message and set the hop count 0 in the hop count field of RREP. If the receiving node is not the destination, then the Destination Sequence Number field in the RREP message will be updated with its known sequence number for the destination. And the forward route entry is updated by putting last hop node into precursor list. A node can receive multiple RREP recommending different paths to the destination node. Then each RREP is examined for the latest route. And the source node only accepts the latest up-to-date path.

Route Monitoring: To conform to the connectivity, each node can broadcast a HELLO message in its active route. The nodes in the precursor list receive the message in a predefined time (not only HELLO message). If any of the messages are not received, then the nodes decide that the particular node is not reachable. After the determination of unreachable node, the node removes all the route entries from its routing table and a RERR message is generated. This RERR message sent to the precursors contains all the nodes that are unreachable due to the breakage of the link. The precursors revise their routing table and send the RERR message further to their precursor.

ADVANCEMENTS IN AODV

As discussed in section I, the bandwidth and mobile device power are two important factors that need to be conserved in order to do the effective communication. With the advent of time, the advancements in the working of the AODV routing protocols are going on. This section is throwing light on the work of some eminent researchers who have worked towards improving the AODV in terms of energy conservation and optimization.

P Nayak, R Agarwal and S Verma [23] projected the algorithm Energy aware routing (EAR) using variable transmission range to make the network energy aware. The algorithm is based on the varying the communication range of the nodes. The authors intended to manage the level of the energy for each packet in a distributed manner at every node, thus influencing the consumption of energy in a network. By selecting the larger transmission range, there would be less number of nodes required. Choosing a higher transmission range reduces the number of nodes needed to reach the final node. But it produces large interference. And if the transmission range is small, the requirement of a number of forwarding nodes will be high with less energy utilization. The authors have only focused on the energy.

May Cho Aye and Aye Moe Aung [24] introduced an energy efficient multipath routing protocol based on AOMDV(Ad-Hoc On Demand Multipath Distance Vector) to decide energy efficient path. In the algorithm, node's transmission power and residual energy are considered to exploit the network lifetime and to decrease the energy utilization of devices during the route establishment between a source and the destination. Two energy metrics (residual energy and transmitted power) are chosen to find the route between a source and the destination. But the algorithm hasn't taken the consideration of security and the route optimization.

S Kumar, S Rana and A Sharma [25] depicted the energy efficient routing protocols for Mobile Ad-Hoc Network (MANET). In this protocol, the only energy of a node is considered.

Jin-Man Kim and Jong-Wook Jang [26] proposed an enhanced AODV routing protocol. The research was intended to enhance the AODV protocol to maximize the networks lifetime. Energy Mean Value algorithm is applied to make the device energy-aware. The protocol has taken the energy as a metric to find the optimum path.

Yumei Liu, Lili Guo, Huizhu Ma and Tao Jiang [27] proposed a multipath routing protocol named MMRE-AOMDV. The algorithm is the extension of AOMDV routing protocol. It always selects the path having a high residual energy of node. It can maintain node's energy utilization and extends the network's lifetime. But the algorithm doesn't provide the optimal route and less attention towards .

Similar way Z. Zhaoxiao, P. Tingrui, and Z. Wenli [28] have proposed the algorithm. In this, a threshold limit is assigned on the energy of a node and the nodes less energy are evaded to increase the lifetime of a node so, the route having a larger capacity and less energy is selected in the algorithm using synthetic analysis. The algorithm has only worked toward making the routing energy efficient.

Nagaraj M. Lutimath, Suresh L, Chandrakant Naikodi [29] have proposed an algorithm named Energy aware multi path AODV protocol (EAMAODV). Three energy metrics (energy of the intermediate node, drop rate, and threshold drop rate) are used in the algorithm. The algorithm has only worked toward making the routing energy efficient.

J. Dowling et al [30] optimized the routing in MANET by using the collaborative reinforcement learning. The routing is optimized by changing the environment based on positive and negative feedback. But bandwidth and power are not optimized.

The agent's view about the neighborhood can be changed in a negative way by the feedback model with a negative feedback and an agent can learn about the effectiveness of actions through collaborative feedback and exchange this learning with each other.

Bilgin, Zeki, and Bilal Khan [31] have proposed the algorithm for route optimization named Shrink. The algorithm is the extension of AODV and works after the route establishment. It minimizes the needless hops on the dynamic route. The energy and bandwidth utilization are not considered in the protocol.

Wu Celimuge, Kazuya Kumekawa, and Toshihiko Kato [32] have proposed the algorithm that is based on AODV which has considered the stability of the network link and the bandwidth efficiency. In the algorithm, the Q-Learning approach is used to find the network state information and the information is used to find the better route. The route selection depends on the no. of hops, link stability and the efficiency of the bandwidth. But the security of the algorithm is not considered.

Kalaiyarasi, V., and M. Tamilarasi [33] also proposed the algorithm for increasing the bandwidth efficiency and effectively exploiting the energy. The algorithm is based on clustering and tried to decrease the retransmissions and thus increasing the throughput and reducing the delay. But the route optimization and security are not considered.

The researchers also worked towards the security of AODV and modified the AODV to make it secure. Karthikeyan, B., S. Hari Ganesh, and N. Kanimozhi [34] have extended the AODV to protect it against link failure, black hole attack, and malicious node intrusion attack.

Rai, Anuj, Rajeev Patel, R. K. Kapoor, and D. S. Karaulia [35] also proposed the algorithm to secure the AODV against black hole attack. But the energy and bandwidth are not optimized in these algorithms.

The dwelling of the literature reflects that the researchers worked towards the one or two parameters for e.g. either making the protocol energy efficient or secure. Very few research works are reported which have taken consideration of the four parameters (Power Conservation, bandwidth conservation, route optimization and security) together. The proposed work is forwarding the attention and providing direction for taking all the challenges together and giving a solution which is based on mobile agents.

MODIFIED AODV PROTOCOL

The existing AODV routing algorithm has been modified to provide a total solution in terms of getting better power optimization, bandwidth conservation, security and path optimization. In MANET, there are limited power resources. All the mobile devices work on battery and it is a challenging task to save the battery for efficient task performance. The proposed algorithm which is power optimized secure mobile agent based AODV (POMA-AODV), is orienting towards this and optimizing the energy through the application of mobile agents in AODV routing protocol. Autonomous and intelligent mobile agents are applied in the algorithm. In the algorithm, the agents carry the RREQ packets with them and find the route between the source and the destination. Whenever the agent reaches to the neighboring node, the agent will check for the destination address. If the address is found in the routing table of the node, then it does the further processing otherwise again the agent move to the next neighbor node. The process continues till the agent finds the destination address. The advantage of using the mobile agent is that the agent works on the disconnected operation. They only require the bandwidth at the time of roaming in the network. And the power of the node is also optimized. Figure 2 is depicting the dispatching of mobile agents by the source node in the network. The proposed algorithm is performing the four tasks:

i. Optimization of the power of a node: As discussed in section II, the mobile agents roam around the network autonomously and can perform disconnected processing. Due to the disconnected operation, the mobile device's power can be optimized.

ii. Bandwidth Optimization: Due to the disconnected operation of mobile agents, continuous bandwidth is not required in between the communicating node, and thus bandwidth can be optimized.

iii. Providing Security: The mobile agent performs the self-healing function, which will not allow the routing through any node that is considering being malicious. In the algorithm, the mobile agent is continuously monitoring the status of every node and when it found the packet drops at any node, it doesn't consider the path that has the particular node on which the packets are dropping. Thus it provides security to the network and a secure communication is provided.

iv. Optimal Path selection: Fourth, the mobile agent will find the optimal path from source to destination through hop count.

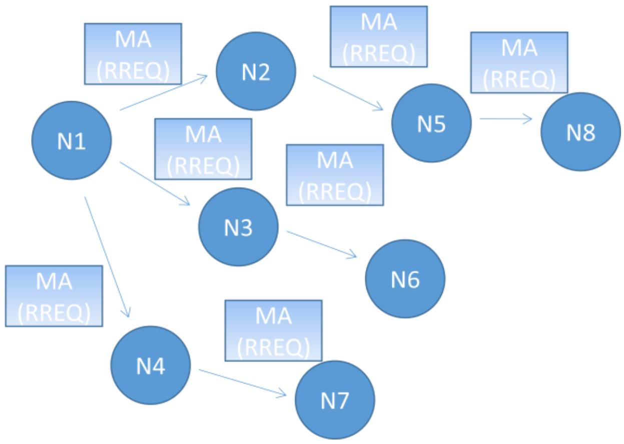

Figure 2: Dispatching the Mobile agents to the neighboring node

The following algorithm is describing the whole process with the revelation of the steps underneath:

Step 1:

Source Node will generate the mobile agents (MA) and the mobile agents shall carry the RREQ packet to the neighboring node. The node will check the RREQ packet.

Step 2:

On the off chance that there is a path between sender to receiver in routing table, value of the receiver sequence number in the section containing the path entry and the receiver sequence number in the packet RREQ will be compared.

Step 3:

On the off chance that the receiver sequence number in RREQ packet is greater than the sequence number in the routing table, it won't utilize path of the steering table to answer to the source node. And the mobile agent will forward ahead with the RREQ packet to the next node and the number of hops will be augmented by 1.

Step 4:

Else, MA will move back with RREP bundle taken from the node to affirm the receipt of RREQ parcel. Along with hop count and TTL. If this is not the case then step 5 will be executed.

Step 5:

On the off chance that there is no sender to the receiver in the routing table, the mobile agent will move forward to the next node with RREQ packet. 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.

Step 6:

The mobile agent will move ahead until reaching to the receiver node or a node whose conditions fulfill step 2.

Step7:

Amid the time multiple mobile agents will come back with RREP parcel, the mobile agent having a largest sequence number and minimum hop count will be chosen and the path is updated in the routing table.

The flow of the algorithm is depicted in Figure 3.

SIMULATIONS AND RESULTS

The simulation is carried out in Network Simulator 2(ns2) [36]. The work is simulated with a map size of 1000m * 1000m. The network layer protocol is TCP. The traffic model is constant bit rate and the mobility model is random way point. Table 1 is summarizing the parameters used for simulation:

Table 1: Simulation Parameter

Parameter	Value
Simulation time	500 s
No. of Nodes	Varying from 10 to 50
Map Size	1000m* 1000m
Mobility model	Random Way point
Traffic Model	Constant Bit Rate/TCP
Transmission Range	250 m
Packet Size	512 bytes

The simulation is done to simulate the proposed algorithm and results were derived according to the following performance metrics:

- Packet delivery ratio:

The packet delivery ratio (PDR) is a ratio of the packets received successfully at the destination node compared with the packets sent by the sender node. It can be calculated as:

PDR = (Total no. of packets received by the destination node/Total no. of packets sent by the source node)*100

In the proposed algorithm the PDR is calculated by varying the number of nodes.

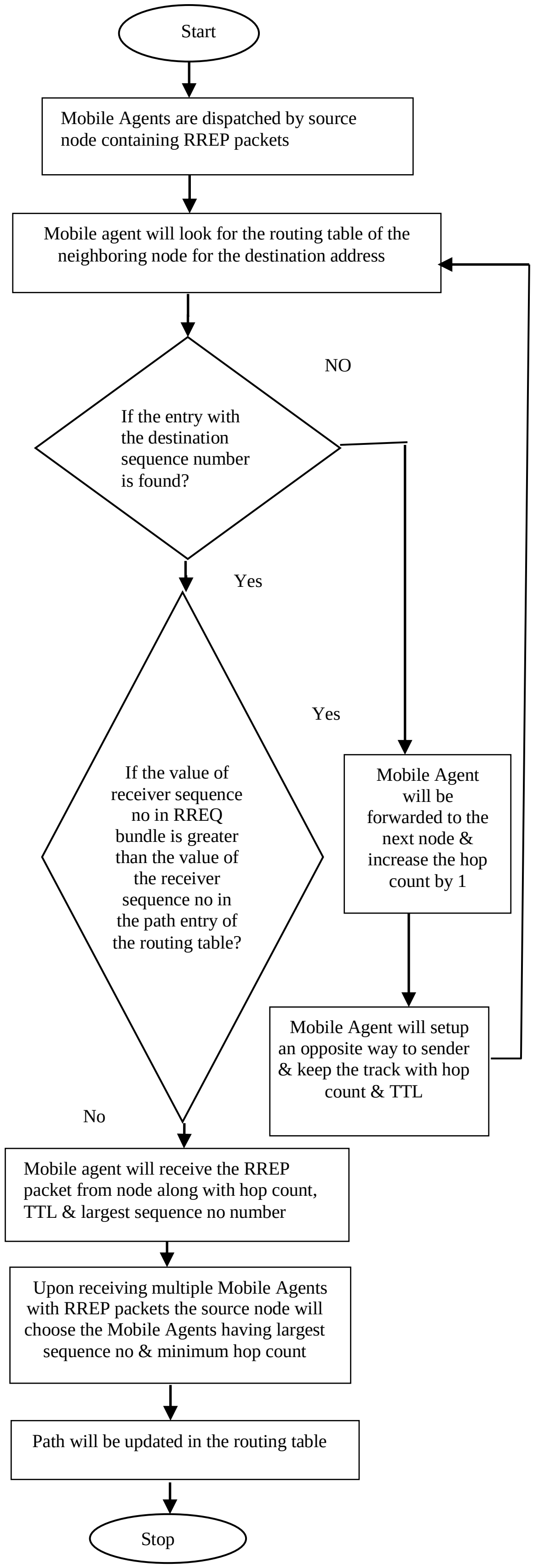

Figure 3: Modified AODV algorithm

The results in Figure 4 show that the PDR of POMA-AODV is high as compared to AODV routing protocol.

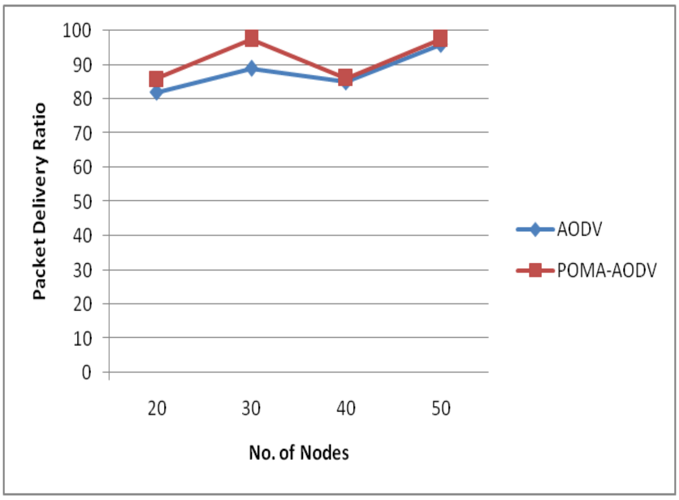

Figure 4: Packet Delivery Ratio with varying No. of Nodes

- Throughput

Throughput is the rate at which the packet is transmitted effectively in a total simulation time. It is defined as the number of data packets transmitted over the total simulation time. It is calculated as:

Throughput= N/1000

Where N is the number of bits delivered to all the destinations nodes successfully.

The graph in the Figure 5 is depicting the high throughput in case of proposed algorithm as compared to normal AODV as the numbers of nodes are increased.

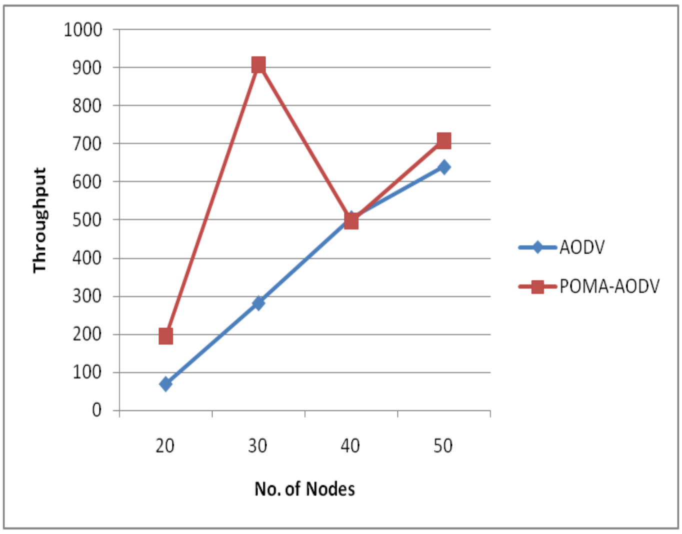

Figure 5: Throughput versus No. of Nodes

- Total Consumed Energy:

It is the sum of energy consumed by all the nodes during a total simulation time. The consumed energy of a node can be calculated as:

Total Energy Consumed during the simulation = $\sum^{n}_{i=0}$ (Node's Initial Energy – Node's Residual Energy)

The graph in Figure 6 depicts that in the proposed algorithm POMA-AODV total energy consumed is less as compared to normal AODV

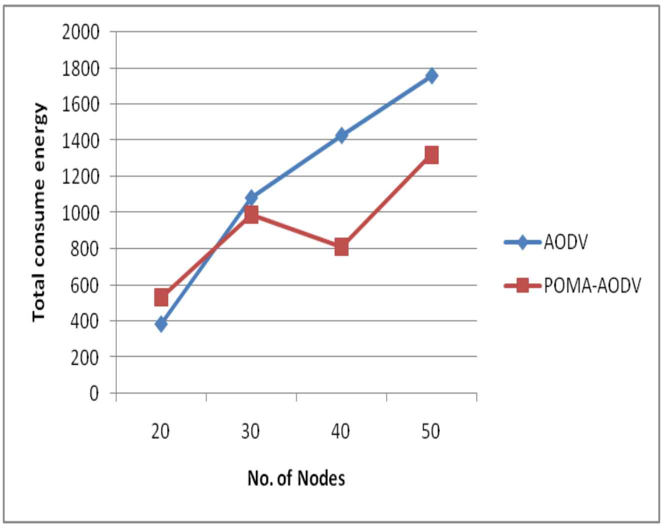

Figure 6: Total Consumed Energy versus No. of Nodes

- Average Energy Consumption:

It is the average energy consumed by each node in the network over a total simulation time which is the average node residual energy. And the graph in Figure 7 is depicting that the average consumed energy is less in case of POMA-AODV as compared to normal AODV.

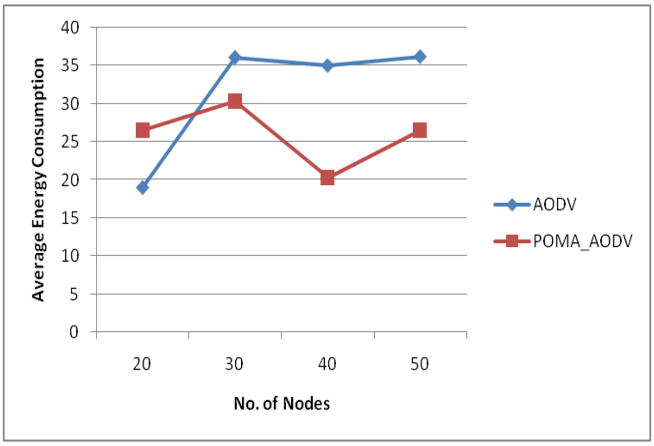

Figure 7: Average energy consumed on each node versus No. of nodes.

- End-to-End Delay

It is the average time a data packet takes to reach from a source to the destination. It includes the delay in processing, delay due to queuing of the packet during congestion and the delay in the transmission. It can be calculated as

End-to-End delay = $\sum$ (packet's arrival time at the destination – Packet's sending time from the source)/Number of packets

As shown in Figure 8, the end-to end delay is low in case of POMA-AODV if compared with traditional AODV.

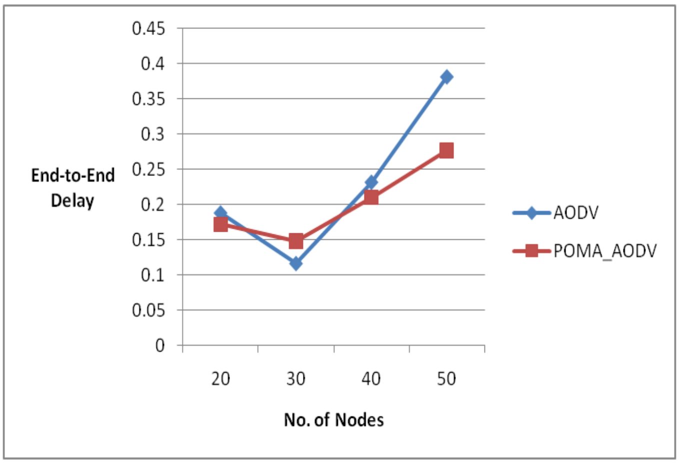

Figure 8: End-to-End Delay versus No. of Nodes

Thus, it is concluding from the results that the POMA-AODV is much more efficient than conventional AODV in terms of PDR, throughput, total energy of all the nodes and the average energy consumed. It shows that the proposed algorithm is more power optimized; bandwidth optimized and provides optimized routing.

CONCLUSION

As the mobile devices work on battery, the devices have limited processing power. So the power optimization is the imperative issue to be handled. The paper studied the current advancements in AODV in context with the power of a node, bandwidth utilization and security. And proposed an algorithm based on mobile agents which optimize the power of the node and bandwidth. It provides the optimal path by selecting the path having minimum no. of nodes. Also, the algorithm is secure as it doesn't include the node having high packets drop rate. The experiment results have shown that the proposed algorithm is consuming less energy as compared to normal AODV, thus making the protocol energy efficient and the high PDR, high throughput and low end-to-end delay in the algorithm proving that the algorithm is bandwidth optimized and provides the optimal path.

REFERENCES

[1] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic,"Mobile Ad-Hoc Networks", book, wiley publication.

[2] S. Murthy J.J. Garcia-Luna-Aceves, "A routing protocol for packet radio networks", in: Proceedings of the First Annual ACM International Conference on Mobile Computing and Networking, Berkeley, CA, 1995, pp. 86– 95.

[3] C.E. Perkins, T.J. Watson, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers", in: ACM SIGCOMM'94 Conference on Communications Architectures, London, UK, 1994.

[4] S. Radhakrishnan, N.S.V Rao, G. Racherla, C.N. Sekharan, S.G. Batsell, "DST—A routing protocol for ad hoc networks using distributed spanning trees", in: IEEE Wireless Communications and Networking Conference, New Orleans, 1999.

[5] D. Johnson, D. Maltz, J. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks", Internet Draft, draft-ietf-manet-dsr-07.txt, 2002.

[6] S. Murthy and J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and Applications Journal, pages 183–197, Oct. 1996.

[7] C. Toh, "Associativity-Based Rotuing for Ad-Hoc Mobile Wireless Networks", Wireless Personal Communications, 4(2):1–36, Mar. 1997.

[8] V. Park and S. Corson," Temporally-ordered routing algorithm (TORA)", version 1 functional specification. Internet Draft, Internet Engineering Task Force, Nov. 2000. http://www.ietf.org/internet-drafts/draft-ietf-manet-toraspec-03.txt.

[9] Alexandre Manguer,"Mobile agents in ad hoc networks", thesis, April 2003.

[10] Samuel Lee, "Mobile Agents", A tutorial report, Agent based software engineering.

[11] I satoh, "Mobile agents," In: Nakashima et al (eds.) Handbook of Ambient Intelligence and Smart Environments, Springer, 2010, pp. 771- 791.

[12] Fuggetta, G. Picco and G. Vigna, "Understanding code mobility," IEEE Transactions on Software Engineering, vol. 24, no. 5, May 1998, pp. 342-361.

[13] Saleh Ali K.Al-Omari1, Putra Sumari, "An overview of mobile ad-hoc networks for the existing protocol and applications", International journal of application of graph theory in wireless ad-hoc networks and sensor networks, vol 2, No. 1, March 2010

[14] L. D'Anna, B. Matt, A. Reisse, T. Van Vleck, S. Schwab, and P. LeBlanc, "Self- Protecting Mobile Agents Obfuscation Report," Report #03-015, Network Associates Laboratories, June 2003.

[15] Nikos Migas, William J.Buchanan, and Kevin A. McArteny, "Mobile Agents for Routing, Topology Discovery, and Automatic Network Reconfiguration in Ad-Hoc Networks", in proceeding of 10th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03)

[16] Annapurna Patil, Saunhita Sapre," Intelligent Energy Efficient Routing Protocol based on Biological Agents for MANETS", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014

[17] Neogy, R.; Chowdhury, C.; Neogy, S., "A reliable service discovery protocol using mobile agents in MANET," Reliability and Maintainability Symposium (RAMS), 2012 Proceedings - Annual , vol., no., pp.1,7, 23-26 Jan, 2012, doi: 10.1109/RAMS.2012.6175451.

[18] Bindhu.R, "Mobile Agent Based Routing Protocol with Security for MANET", International Journal of Applied Engineering Research, Dindigul Volume 1, No1, 2010

[19] N. Minar, K.H. Kramer, and P. Maes, "Cooperating Mobile Agents for Dynamic Network Routing", MIT Media Lab, http://xenia.media.mit.edu/~nelson/research/ routes-book chapter/minar.pdf, Software Agents for Future Communication Systems, 1999, ISBN: 978-3-642-63584-7 (Print) 978-3-642-58418-3 (Online), pp 287-304, doi: 10.1007/978-3-642-58418-3_12

[20] Gray, Robert, David Kotz, Saurab Nog, Daniela Rus, and George Cybenko, "Mobile agents: The next generation in distributed computing." In Parallel Algorithms/Architecture Synthesis, 1997. Proceedings., Second Aizu International Symposium, pp. 8-24, IEEE, 1997.

[21] Sultanik, E., "Secure Mobile Agents on Ad Hoc Wireless Networks." The Fifteenth Innovative Applications of Artificial Intelligence Conference Acapulco, Mexico, 2003.

[22] Perkins CE, Royer EM, Chakeres ID 2003, "Ad hoc On-Demand Distance Vector (AODV) Routing". IETF Draft, October, 2003, available at http://tools.ietf.org/html/draft-perkins-manet-aodvbis-00. Accessed 21 February 2008.

[23] Pinki Nayak, Rekha Agrawal and Seema Verma," Energy Aware Routing Scheme for Mobile Ad Hoc Network Using Variable Range Transmission", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.4.

[24] May Cho Aye and Aye Moe Aung, " Energy Efficient Multipath Routing for Mobile Ad Hoc Networks", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3,2014.

[25] S. Kumar, S. Rana, A. Sharma, " Energy Efficient Routing Techniques for Mobile Ad Hoc Networks", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359,Vol.3, Issue-8,2014.

[26] Kim, Jin-Man, and Jong-Wook Jang. "Aodv based energy efficient routing protocol for maximum lifetime in manet." Telecommunications, 2006, AICT-ICIW'06, International Conference on Internet and Web Applications and Services, IEEE, 2006.

[27] Liu, Yumei, et al. "Energy efficient on-demand multipath routing protocol for multi-hop ad hoc networks." Spread Spectrum Techniques and Applications, 2008 IEEE 10th International Symposium on. IEEE, 2008.

[28] Zhaoxiao, Zhang, Pei Tingrui, and Zeng Wenli. "Modified energy-aware AODV routing for ad hoc networks." In Intelligent Systems, 2009, GCIS'09, WRI Global Congress on, vol. 3, pp. 338-342, IEEE, 2009.

[29] Nagaraj M. Lutimath ,Suresh L ,Chandrakant Naikodi, "Energy Aware Multipath AODV Routing Protocol for Mobile Ad hoc Network" , International Journal of Engineering Research ISSN:2319-6890 Volume No.5, Issue Special 4, pp : 790-991

[30] Jim Dowling, Eoin Curran, Raymond Cunningham, and Vinny Cahill, "Using Feedback in Collaborative Reinforcement Learning to Adaptively Optimize MANET Routing", IEEE Transactions on Systems, MAN, and Cybernetics—Part A: Systems And Humans, Vol. 35, No. 3, May 2005.

[31] Bilgin, Zeki, and Bilal Khan. "A dynamic route optimization mechanism for AODV in MANETs" IEEE International Conference on Communications (ICC), 2010.

[32] Wu, Celimuge, Kazuya Kumekawa, and Toshihiko Kato, "A MANET protocol considering link stability and bandwidth efficiency." UltraModern Telecommunications & Workshops, 2009. ICUMT'09. International Conference on. IEEE, 2009.

[33] Kalaiyarasi, V., and M. Tamilarasi, "Optimized Clustering Mechanism for Qos Aware Route Discovery in Manet." International Journal of Computer Science and Engineering 4.2 (2016): 1372-1377.

[34] Karthikeyan, B., S. Hari Ganesh, and N. Kanimozhi, "Security Improved Ad-Hoc on Demand Distance Vector Routing Protocol (SIm AODV)." International Journal on Information Sciences and Computing 10.2, 2016.

[35] Rai, Anuj, Rajeev Patel, R. K. Kapoor, and D. S. Karaulia, "Enhancement in Security of AODV Protocol against Black-hole Attack in MANET" In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, p. 91, ACM, 2014.

[36] NS-2 with Wireless and Mobility Extensions, available via web-site http://www.monarch.cs. cmu.edu.