SDVCA – A Robust and Secure Data Communication Protocol for Manet

Anusha Kannan (knu.anusha@gmail.com)
School of Computer Science and Engineering https://orcid.org/0000-0002-8391-1744
Manikandan N
VIT University School of Information Technology and Engineering
Mallikarjuna Nandi
Rajiv Gandhi University of Knowledge Technologies
Morsa Chaitanya
RVR and JC College of Engineering
Chunduru Anilkumar
GMR Institute of Technology Department of Information Technology

Research Article

Keywords: Mobile Ad hoc Network (MANET), Software Defined Networking (SDN), Delay Tolerant Networking (DTN), Virtual Certificate Authority (VCA).

Posted Date: October 28th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-989798/v1

Abstract

The existence of intruders is a threat factor in any network. Degradation of the network operation occur which include delay in transmission, reduced network energy level, low throughput and many. In heterogeneous networks, the threat is complex since it has several interconnected devices working with different operating systems. To solve the trust dispute in the network a Robust and Secure Data Communication Protocol for MANET termed as Software Defined networking enabled Virtual Certification Authority (SDVCA) is proposed. In MANET, the nodes forward information among them. To control the data flow in a MANET the network has to establish a controller node and forwarder nodes for transmitting or forwarding data. The forwarder node carries out the operation of router. The VCA provides authentication certificate for all the network nodes. Without this authentication, the node will be declared as an untrusted intruder. No data will be transferred to or through them. Hence a trusted network is formed and efficient safe data transfer is achieved. In the proposed scheme, the control logic of MANET is moved from forwarding plane (node) to control plane (node) for improving the network performance. A social network model in MANET is designed to create controller-based architecture. This controller node will function as a host and also as a pathway of connecting different social networks in MANET architecture. The results provide improved performances and the network has better throughput, and lesser end to end delay when compared with the existing techniques.

I. Introduction

Group of interlinked components are termed as network. Example of such network is sharing of data, application and machines like scanners, photo copiers by the computers in the office. Local Area Network (LAN) is the topology of connecting various systems together inside a restricted area like office, house. Work Groups are the component of a huge LAN. Various work groups are coupled through the device called router. Hub and switches are connecting devices that unite network members. Router, a connecting device which connects networks together. The networks discussed so far are stationary and are connected with LAN cables. Alternatively the technically evolving network termed as MANET is the center of discussion. As the name suggests, the network devices that exchange information’s are mobile in nature. Every node in the MANET is able to function as a host, router and recipients.

When comparing the conventional wireless communication, MANET is applicable in military grounds. Permanent wireless communication bases cannot be established in the drastic war situations. The soldiers and the trucks require dynamic information updates for timely plan execution. To meet the critical requirements, MANET is employed. In catastrophe conditions like earthquake, tornado, tsunami calamities the available communication facilities would have been destroyed. To establish good communication in critical conditions, MANET is employed. In isolated locations, communication to the outside locality is achieved with MANET[1]. To achieve efficient wireless network, sensors are used. Usually the sensors have short lifetime. So it is used with MANET by adopting multi hop technique of the ad hoc to achieve communication.

SDN is developed to control the network functionality. Basically the network devices like routers and switches contains two planes namely the Control Plane (CP) and the Forwarding Plane (FP). The CP has the instructions for the operation of the FP. Data encapsulation, de-encapsulation and selecting optimal path for data transfer are the task of FP. Network equipment configuration is done by Command Line Interface (CLI). But it is a tedious task to configure an entire network due to its complex commands Thus SDN is preferred for configuring any network owed to its simplicity. Open Flow is the popular SDN protocols used which operates in three layers. They are the infrastructure layer, the control layer and application layer. The Infrastructure Layer is responsible for forwarding data packets. The Control Layer sustains the network status such as node status, link status, and network topology. The Control Layer transmits the matched flow tables to devices in the network over the southbound interface (Data Forwarding Plane and Control Plane Interface) and delivers information to the upper layer over the north bound interface (Control Layer and Application Layer Interface). DTN are network architectures that addresses technical faults found in the heterogeneous networks. The network of components working with dissimilar operating systems in them are called heterogeneous system. DTN could not apply or use the MANET protocols. Because, MANET protocol works on the basis that numerous path exists among any pair of source and destination[2]. But those paths are not permanent because of the frequent mobility of nodes.

Therefore network performance is degraded and life time of node is also reduced. To enhance the network performance, a novel trust establishment for MANET is proposed. A social network is modelled in MANET to create controller based architecture is shown in figure 1. In this network, all nodes act as router as well as host. The proposed techniques chooses a MANET node as the controller, which is present in the network for a long duration. The controller or another host can be a gateway to connect another social network.

The section II surveys the existing techniques of MANET. Section III offers the specifics of the proposed a novel technique of SDVCA for MANET. The performance of the planned technique is estimated in section IV. Finally the article is concluded and the enhancement that will be implemented in future is stated in section V.

Ii Related Works

This section furnishes the overview of the existing concepts which led to this proposal. During disaster conditions the information should be transmitted to all network members. Multicasting was needed to meet the requirement. The energy of the node was lost faster in multicasting. This resulted in transmission loss. Roy, et al. [3] Proposed a technique of selecting relay in DTN for multicasting single and multiple data transmission during disaster conditions. The relay or node with good energy level in the network was selected. The life of the network was increased by the scheme. The shortest path for forwarding information was selected to improve message delivery time. The technique required optimal improvement in node energy preservation. In the previous technique congestion control was not focused. Roy, et al. [4]Planned a technique of congestion aware DTN multicasting which selected only

minimum relays for transmission process. It saved buffer space. The node mobility and its energy level was considered for network life and communication efficiency. High energy was lost when node mobility was high. Network life time decreased in proportion to the node energy. To improve network efficiency Tan, et al. [5] modelled a Signal Efficient Clustering Algorithm (SECA). Based on the signal strength at every node of the MANET the most stable node was selected as the Cluster Head (CH). CH overlapping was prevented to achieve un-collapsed information transfer and less path complexity. With higher node mobility, the life of CH was low. But the proposed algorithm selected a node with high signal strength reception and frequently changed the CH based on signal strength. Thus the CH life duration was improved. MANET reliability was dependent on the node position in the network region. Without prior knowledge of the node in a terrain it was difficult to configure the nodes. Gundry, et al. [6] Offered Differential Evolution (DE) based DTN for MANET. For establishing MANET, every node determines its position in the terrain by executing the TCM-Y algorithm. It also adjusts it position and also maintains its connectivity or path with its k neighbors by using Yao graph. It was used in unmanned vehicles, GPS. Development was focused to implement the scheme in underwater node positioning. In most wireless networks, many unregistered nodes enter and the level of data security decreased. Kushwaha and Lokhande [7] Framed a unique method to develop the MANET's security by detecting intrusions. Future work was based on increasing and managing the number of users in network in order to build network strength. The wireless nature of the MANET was suspicious to be attacked by various attacks such as black hole attack, wormhole attack. Kaur and Singh [8]Designed a technique to determine wormhole attack. A node was used as a bait for such attack. Further optimization to detect intrusion was required, because data could be lost before executing the prevention algorithm. The existing scheme of VANET faced connectivity issues and had poor accuracy. Truong, et al. [9] Recommended an SDN based Fog computing to effectively deploy network services in VANET. Vehicle - vehicle, vehicle - infrastructure and vehicle - base station communications were augmented for effective connectivity. Future work was focused to extract details of base station, and to optimize data forwarding rules. The rapid wireless communication growth required the technology MANET. Multimedia data transfer required an improvement in quality of service. Mahadevan [10] Proposed a scheme to enhance the performance of the network to meet the multimedia service requirement. A channel was modelled to extract the path loss and gain. Queuing model was developed to estimate the delay in transmission. Based on the estimates from the model, the network throughput was increased to improve QoS. Further development was to improve QoS under varying environmental conditions. Data security was always a challenging task. In traditional schemes, either the path routing or the data security is considered. Ahmed, et al. [11]Designed a frame work for MANET based on flood factor. Every node in the MANET was validated by grey wolf algorithm and optimal path was selected by multi swarm optimization. Future development was to enhance throughput in MANET. The routing protocols routed the data based on the shortest path. In addition the available battery power of the node need to be considered for effective data transfer. Bade, et al. [12]Framed an energy aware algorithm to adopt the appropriate path with sufficient energy levels at the nodes. The scheme improved the life of data path. End to end delay was significantly higher and hence improvement was focused to enhance delay at ends. Wireless networks were lossy due to channel interference and fading. Chen, et al. [13] Planned a multicast routing protocol to reduce bandwidth

consumption of unnecessary data. Development work was based on optimal resource utilization and improvement in QoS. Space researches and other intensive operations implied Delay / Disruption Tolerant Networking. The delay and latency of data transfer was present in all operating conditions of DTN. A clear estimate of the delay timing was required to achieve efficient data transfer control. RTT (Round Trip Time) model for DTN protocol was designed byYu, et al. [14]. Performance analysis on the convergence Layer of DTN was executed. File transfer experiments were conducted to validate the model. The delay was reduced when a packet size greater than the threshold limit is transferred. Future development was concentrated on improving RTT. Previously the Geographic Routing schemes were applied to homogenous scenarios. Cao, et al. [15] Proposed the Best Geographical Heterogeneous Relay Routing (BGHRR) scheme for heterogeneous scenarios with identical node mobility and varying node mobility. The data delivery was higher than the homogenous modes. Development was needed to improve transmission delay in dynamic conditions. With all improvements to deliver high quality of service, Wang, et al. [16] surveyed the geographical routing of DTN and the challenges in its deployment. The DTN in Vehicular Sensor Network faced frequent interconnection issues. Besides predicting the faults the optimal routing technique needed to be framed. To effectively replicate the message to nodes of successive energy levels Cao, et al. [17] modelled a three phase operation of Encounter Based Routing Framework (EBRF). Future investigation was focused to dedicated encounter prediction. Network traffic was critical criteria faced by the nodes while transmitting data. The peak sessions of the paths and link capacity was unknown by the senders in order to avoid delay in transmission. Basit, et al. [18] Designed a cross layer coordinated multipath forwarding scheme glued in along SDN to achieve reliable and increased throughput. Route traffic was controlled by extracting parameters of the links capacity, peak sessions in the paths. Future work was to improve throughput under conditions when new nodes were added. Power management of cloud data centers was required to be maintained for effective network reliability. More than 10 to 20 percent of power is consumed by the network. SDN is preferred for network traffic and improving QoS. Resource overbooking on one host to reduce the active number of hosts met the power requirement. Son, et al. [19] Organized a dynamic overbooking strategy with SDN. It could over book a host and network and minimized Service Level Agreements (SLA) violations. Mobile networking based on SDN was in the development stage. The increase in smartphones and service application increased network traffic in LTE mobile networks. Nguyen and Kim [20] Designed an Open flow Enabled mobile Packet Core networks (OEPC). The SDN open flow protocol was used for path management, mobility management, tunnel management. The signaling cost was lower than traditionally used techniques. Future work was based on distributed mobility management. Sleep scheduling mechanism was needed to manage node energy to improve network life time. All available node in the network was awake at all the time even if they were not required for data transmission. These idle nodes consumed more energy of the network. Hence an effective algorithm was required to shut down idle nodes and activate them when needed. Previous method used beacon data which was transmitted from all nodes to the controller at particular intervals for updating their status and instruction request. But that technique consumed more network energyWang, et al. [21] proposed an SDN based Sleep Scheduling algorithm. (SDN-ECCKN). It was executed in the controllers alone. The algorithm switched off the nodes by calculating their residual energy. Future work was based on managing network energy when new nodes

were added frequently. Multicasting was the method of transmitting the same message to different destinations. In Existing technique, the data centers included inactive or failed links for multicasting. That was inefficient method and less robustive. Zhu, et al. [22] Provided a multicast solution for SDN based Data centers. Multicast group manager was formed to schedule the multicast flow between active links. The proposed technique bypassed inactive links to achieve high efficiency and robustness of resource multicasting. Future improvements was focused to enhance throughput in network while maintaining robustness. The network traffic increased whenever new services was introduced. Nguyen, et al. [23] Presented a virtual LTE mobile network with a general SDN architecture to understand the issues that arose in the network topology. The scheme required careful selection of network operators to provide service based on financial and methodical benefits. SDN was flexible technology that grew fast. Virtualization of an SDN network Blenk, et al. [24] surveyed a hypervisor to virtualize SDN. A hypervisor permitted multiple users to access the physical SDN network by slicing the network and split it in to numerous virtual SDN. The results was beneficial. More research was required to improve the virtual SDN performance. . The communication paths was uneven and the network structure changed more frequently in vehicle based network. Park and Yoo [25] Proposed fog computing and SDN to solve the imbalance. Highly complex failures in fog servers and multi- hop network patterns need to be focused in the upcoming work.Sundar, et al. [26] Designed Zigbee based protocol to test MANET. The throughput of MANET was tested by letting the nodes to be in continuous mobility. The test environment was a small car parking lot and the throughput gave varying data's. The testing needed to be expanded to large MANET conditions throughput also needed to be maintained stable.Garcia-Luna-Aceves [27] Investigated MANET routing protocols. Real time data was used in the network simulation instead of using default simulator values. Further drastic network parameters need to be implanted for testing the MANET. The scalability of a MANET was improved by clustering technique. But such clusters should be protected from malicious attacks. Bidaki and Masdari [28] Framed a reputation based clustering algorithm and established a trust bound cluster. The scheme had to be tested on hostile environments. Information broadcasting to various neighbors in the network was applied in wireless ad hoc networks and sensor networks. Rashid, et al. [29] Provided a broad overview about various broadcasting strategies. The disputes faced in the broadcasting policy was presented. Next stage research was intended to frame a novel strategy to broadcast information. A robust MANET establishment was required to allow distributed applications to exchange data without interruption.Detti, et al. [30] Developed a topic based publish subscribe structure to provide reliable and fast data exchange. Next phase of development was focused to manage the network subscribers and verify the transmitted data to enhance network trust.

Iii Proposed Method

In the proposed technique of SDVCA, a secure data heterogeneous MANET is formed by verified and trusted nodes. Since all nodes possess no prior knowledge of others, they have to be provided with authentication certificates and trust certificates. In a heterogeneous network, the trust establishment of all the nodes in the MANET is performed by VCA based Mutual Authentication scheme. The components of

VCA are Trust Initiator, MANET Node, Cluster Certificate Authority, Global Virtual Certificate Authority and Cluster Virtual Certificate Authority.

Trust Initiator (TI):

The SDN controller node of the MANET serves as the TI. It is responsible for forming the secure MANET. It contains the certificate signed by the GVCA and the certificate of the GVCA itself.

MANET Node (MN):

It is a wireless node that is ready to link and function under an SDN -MANET.

Cluster Certificate Authority (CCA):

A group of MN forms a cluster. There can be numerous clusters in a MANET. CCA is the cluster head which is also a MN. It is a third party node that bridges the TI and MN.This can examine any node in its cluster for its reliability.

Cluster Virtual Certificate Authority (CVCA):

It is the certifying authority unique to each cluster of the MANET. The CVCA signs the certificate for MN and CCA before deploying them into the network. MN and CCA saves their certificates along with the certificate of CVCA. But the private key of CVCA is not revealed to any devices in MANET.

Global Virtual Certificate Authority (GVCA):

It is the certifying authority unique to the MANET. It is the trusted third party between the TI and CCA. GVCA signs the certificate of authenticity for TI and CCA. After certifying them, the certificate of GVCA along with the signed certificates are stored in CCA and TI devices. The private key of the GVCA is not revealed to any devices of the MANET

The work flow of the proposed technique is given in fig 2. In the proposed technique, deployment of all nodes are initiated at the beginning. These nodes are mobile devices that transmit and receive data. They may be located in various locations and may be in disaster conditions. In order to communicate to other devices the node sends a path request to the controller. The controller examines the network for available paths. The controller node has to examine the forwarder node to necessitate successful data transfer. The evaluation of the forwarder node is based on transferring speed, data forwarding and data reversal. The trust value is attained by all the nodes based on the success rate of data transfer. These values are frequently updated in the trust value table. The forwarder node with greater trust value is selected by the controller node. After successful completion of data transfer, the status of the path is updated to the controller. Based on the path details that is updated, the controller decides optimum path for subsequent data transfer. The route that is chosen for data transferring is maintained for allocating resources in the future.

VCA Functioning:

There are two root CAs available in the VCA infrastructure. They are GVCA and CVCA. The GVCA is level-I root CA whereas CVCA is level -2 root CA. The GVCA is responsible for forming initial trust in among TI and CCA. The CVCA is responsible for forming initial trust in between the CCA and MN. The motive of allotting two tier control with different root CA is to provide higher degree of control and trust management to individual clusters in MANET. Thus the communication in heterogeneous networks are successfully managed by utilizing the VCA basedMANET. The integration of the VCA infrastructure to heterogeneous MANET is furnished in fig2. The GVCA is a virtual third party entity. It is unique for every MANET. It contains a private key, which is not revealed to any device inside and outside the MANET. To establish a secure MANET, initially the TI and the CCA has to mutually authenticate each other for participating in the MANET. Algorithm I illustrates the steps involved in the mutual authentication of CCA and TI.

Algorithm I: Mutual Authentication of CCA and TI

Step 1 : GVCA gives the public key and authentication certificate to TI.

Step 2 : GVCA provides public key to CCA.

Step 3 : The CCA requests the certificate from TI for joining the network.

Step 4 : TI sends the certificate to CCA.

Step 5 : CCA verifies the certificate with the public key provided to it by GVCA.

Step 6 : CCA uses the public key of TI to encrypt a nonce and sends it to the TI.

Step 7 : TI replies with the nonce by encrypting it with the public key of CCA.

Step 8 : CCA compares the two nonce and if both matches, then it confirms that the authentication certificate is sent from the original TI.

Step 9 : CCA joins the MANET.

Initially the GVCA provides its public key and signed certificates to CCA and TI. Upon receiving the certificates the TI and CCA starts to mutually authenticate each other. CCA request the certificate from TI for verification. The public key is used by the CCA to verify the authenticity of the certificate provided by TI. Similarly the TI requests the certificate of CCA and verifies the certificate with the available public key for its authenticity. The CCA and TI challenges each other by sending an encrypted nonce. Encryption is done using the public key. At both ends the decryption of the nonce is performed by the same public key. The response task is executed next. The decrypted nonce is encrypted again with the available public key and retransmitted. The TI and CCA compares both the nonce (sent and received) for equality. If the result is true then the mutual authentication is successful. The CCA and TI are authorized to join the MANET.

Mutual authentication between MN and TI has to take place next. Algorithm II provides the steps involved in MN and TI mutual authentication. The CCA and TI are previously authorized as trusted members to control MANET formation. The MNs have to join the CCA to form a MANET.

Algorithm II: Mutual Authentication of MN and TI

Step 1 : CCA authenticates TI and sends network association request.

Step 2 : TI authenticates CCA and associates it in the network.

Step 3 : MN request CCA and CVCA certificate from TI

Step 4 : TI requests the certificates from the CCA device.

Step 5 : TI forwards the certificate received from CCA to the MN.

Step 6 : The MN verifies the certificate of CCA for authenticity and authenticates it

Step 7 : MN requests TI's authentication certificate signed by CCA from TI

Step 8 : MN sends its authentication certificate signed by the CVCA to TI.

Step 9 : TI sends MN's certificate to CCA for verifying MN.

Step10 : If verification is successful, TI approves association of MN with MANET.

The virtual third party entity termed CVCA signs an authentication certificate and sends it to be saved in the CCA and MN devices along with its own certificate. The MNs have to authenticate CCA before linking. Since the addition of any new node into the MANET has to be carried out abiding the governance of the TI, the MN requests the certificate of CCA from TI. This process is done to eradicate the intrusion of unauthorized nodes which will work as false CCA and deviate the MANET's transfer architecture. It requests the certificate from CCA and forwards it to the MN. The certificate is verified by MN and it authenticates CCA. The MN requests the certificates of TI from CCA and TI requests CCA to verify the certificates of MN. If the verification is successful, the MN is permitted to link with the CCA. Hence a MANET is established under trusted conditions.

In the VCA infrastructure, the MN and CCA should be able to request a certificate, verify the signature on a certificate as well as participate in a challenge and response procedure. The CCA should be able to sign a certificate. For which it needs to securely store its private key locally in its Secure Elements (SE) or Trusted Platform Modules (TPM) of the device.

Requesting a Certificate

Certificate request can be started by the MN or a CCA from the TI to join the MANET.

Verifying a Certificate:

To verify a certificate, it is necessary that the data present in the certificate must be correct and trustable. The new and old public key of CVCA, GVCA and CCA are utilized for verifying the certificate.

Challenge and Response:

After the verification of the certificate, the process of challenge and response is essential to guard against a replay attack. In which the intruder can obtain he certificate by snooping. Hence a challenge and response technique like encrypting a public key and private key decryption of nonce, can be employed for verifying the true ownership.

Signing a Certificate:

The MN sends an appeal to CCA to sign its certificate. But the MN is still not authorized node in the MANET. Hence the CCA has to authenticate MN first. After authenticating process, the CCA will sign the certificate of MN.

The VCA infrastructure for the MANET can be implemented in configurations of centralized controller with controller replication and external infrastructure network. The Controller node is the core of MANET which performs the function of TI. It can be configured by the certificates signed by the GVCA. The MN and CCA are configured by the Cluster Administrator (CA) by using the CVCA signed certificates. The CCA contains the certificates that is signed by the GVCA and also has the certificates signed by CVCA. The SDN MANET contains a controller with the support of replication and external network infrastructure. There are two options available for authenticating a. Public Key Interface (PKI) is relied initially. The external network infrastructure discharges the work load of retaining PKI from SDN MANET. The SDN controllers may also be sub-divided into Master Controller (MC) and some Secondary Controllers (SCs). The CCA and MN of a cluster will validate and link with SC in which the TI is located. The MC too runs as a TI and verify with the SC. The certificates which is signed by the GVCA is utilized to configure the available controllers. These certificates are saved in the devices itself. When an attempt is made by a fresh MN to link with a MANET, it must authenticate a TI and must get authenticated by a TI. The chosen TI is situated in the network in which the CCA of the new MN is present. In such a situation, the authentication can progress in a straight forward manner. In case the new MN is not able to straightly contact the chosen TI then the message regarding the certificate request will be forwarded to the chosen TI, CCA and the closest TI instantaneously. At this instant the mutual authentication with the nearest TI is accomplished by the MN with the assistance of the chosen TI and CCA. In certain circumstances where a MN tries to shift present SC to other, it has to change its link from TI also. For this process two modes are offered. The first offer is that the MN does not require to get any authentication for linking with a new SC/TI, since the MN has already been authenticated to be a member of the MANET. But the new SC/TI will verify the reliability of the MN with its previous TI/SC through the MC/TI. The second offer is shifting MN must go through a fresh process of receiving mutual authentication from the new SC/TI with which it going to get linked. The procedure is similar to the method followed by a new MN to join the MANET

The SDN controllers are completely dispersed and every single controller is accountable for a subgroup of the nodes. The controllers will perform the function of TI. The GVCA will sign the certificates of the participating TI and all TI are configured based on the certificate. The certificates obtained from the GVCA are stored in the device itself. If the new MN endeavors to link with the MANET, it is required get mutual authentication with the TI. Based on the location of new MN, it is able to mutually authenticate with the local TI incase its CCA is associated with the TI. If the CCA of the new MN is not linked with the local TI. The MN can obtain mutual authentication through the local TI to acquire the certificate of the CCA that moved. In the same way, when an MN desires to link with another TI, the MN requires the two options of following the MC and SC technique described before.

The advantages of VCA infrastructure are furnished as follows. The nodes experience limited overhead because the certificates of the device alone is saved in the secure elements or trusted platform modules of the nodes before deploying them in the network. The network becomes flexible because, the nodes which are once configured, authenticates themselves when approached by other nodes. This flexible property facilitates the effective communication among heterogeneous platforms.

Iv Performance Analysis

In this section, the performance results of both proposed SDVCAand existing techniques like Energy Aware Multiple Data Multicast (EAMDM), EPIDEMIC[31]and Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET)[32] are analyzed and evaluated based on Packet Delivery Fraction, Throughput, Routing Overhead, Energy Consumption and End to End Delay.

A Packet Delivery Fraction

It is the ratio between the total number of packets received and sent. Figure 3 represents the plot between the simulation time and packet delivery fraction. It is apparent that as the simulation time increases, the ratio decreases because the data packets sent and received decreases as time increases.

The Packet Delivery Fraction is higher than that obtained by using existing techniques as simulation time increases. This indicated the success rate of data transfer

B. Throughput

It is the rate of successful message delivery in the network. The total bytes transferred per second is higher than the conventional methods.at any simulation time.Fig 4 furnishes the plot drawn between the obtained throughput by utilizing conventional method and is can be compared with the result obtained from conventional methods.

C Routing Overhead

It is the amount of information sent in the network by using a portion of the network bandwidth. Fig 5 represents the routing overhead achievement over simulation time. It is clear that the proposed

technique has superior routing overhead than the traditional schemes.

D Energy Saving

The network life time is dependent upon the energy level of the nodes. It is obvious that as time increases the energy of any device decreases. By using the proposed scheme of path selection, the energy level of nodes is saved when compared to the previous techniques.Fig 6 represents the graph against energy saved in the network and total number of nodes.

E End to End Delay

The speed of data transfer is based the delay of data reception. If the delay is high then the receiver interprets the data at an inappropriate time which does not serve the purpose of data transfer.

V Conclusion

Data transfer in evolving with technology. Optimal utilization of communication systems meet the need of the hour. Some communication devices are stationary, but the smart devices that is used in present condition have high mobility. Networking of devices has also evolved from wired mode to wireless mode. SDN for physical routers and networks were undergoing optimal development. Similarly the routing procedures are also developed for secure mobile networks. The proposed technique utilizes a novel VCA to provide reliable and fast data transfer in MANET. The algorithm allots trust certificate to all the nodes that are participating. Before every transmission, the devices exchange their trust certificates and on the basis of trust value, the data transmission begins. The data forwarding and reversal rate at every node is saved in the device itself. The controller node verifies this success rate at all nodes and selects the best node for data transfer. If certificated authentication of any node is failed, then that node will be unassociated from the network. In the similar way, any faulty nodes will also be also neglected since they do not respond to the controller's request for authenticity. The proposed technique enables fast information transfer by reducing the end to end delay. All inactive and nodes with lesser energy levels are eliminated. When the total node quantity of the network increases, an overall improved energy conservation is provided by the proposed scheme by selecting the optimal nodes for allocating resources. The network life is thus increased. Network performance based on throughput, overhead, and packet delivery fraction gives improvements than the conventional techniques such as EAMDM, EPIDEMIC and PROPHET.

Declarations

We, confirm that this work is original and has not been published elsewhere nor is under consideration for publication elsewhere.

Funding:

Not applicable

Conflicts of Interest:

Not applicable

Availability of data and material:

Not applicable

Code availability:

Not applicable

References

[1] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK—a secure intrusion-detection system for MANETs," IEEE transactions on industrial electronics, vol. 60, pp. 1089-1098, 2013.

[2] C. Atheeq and M. M. A. Rabbani, "Secure Data transmission in integrated internet MANETs based on effective trusted knowledge algorithm," Indian Journal of Science and Technology, vol. 9, 2016.

[3] A. Roy, S. Bose, T. Acharya, and S. DasBit, "Social-based energy-aware multicasting in delay tolerant networks," Journal of Network and Computer Applications, vol. 87, pp. 169-184, 2017.

[4] A. Roy, T. Acharya, and S. DasBit, "Social-Based Congestion-Aware Multicast in Delay Tolerant Networks," in Proceedings of the ACM Workshop on Distributed Information Processing in Wireless Networks, 2017, p. 5.

[5] X. Tan, Z. Xiong, and Y. He, "Signal attenuation-aware clustering in wireless mobile ad hoc networks," Journal of Networks, vol. 8, pp. 796-803, 2013.

[6] S. Gundry, J. Zou, M. U. Uyar, C. S. Sahin, and J. Kusyk, "Differential evolution-based autonomous and disruption tolerant vehicular self-organization in MANETs," Ad Hoc Networks, vol. 25, pp. 454-471, 2015.

[7] S. Kushwaha and V. Lokhande, "Security in Wireless Mobile Ad-Hoc Network Nodes Using Novel Intrusion Detection System," International Journal of Engineering Science, vol. 3352, 2016.

[8] H. Kaur and S. Singh, "Wormhole Attack Detection and Prevention in MANET Using Bait Scheme," International Journal of Engineering Science, vol. 11640, 2017.

[9] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, 2015, pp. 1202-1207.

[10] G. Mahadevan, "A combined scheme of video packet transmission to improve cross layer to support QoS for MANET," Alexandria Engineering Journal, 2017.

[11] M. N. Ahmed, A. H. Abdullah, H. Chizari, and O. Kaiwartya, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs," Journal of King Saud University-Computer and Information Sciences, 2016.

[12] S. Bade, M. Kumar, and P. Kamat, "A reactive energy-alert algorithm for manet and its impact on node energy consumption," International Journal of Computer Applications, vol. 71, 2013.

[13] Y.-H. Chen, E. H.-K. Wu, and G.-H. Chen, "Bandwidth-Satisfied Multicast by Multiple Trees and Network Coding in Lossy MANETs," IEEE Systems Journal, 2015.

[14] Q. Yu, R. Wang, K. Zhao, W. Li, X. Sun, J. Hu, et al., "Modeling RTT for DTN protocol over asymmetric cislunar space channels," IEEE Systems Journal, vol. 10, pp. 556-567, 2016.

[15] Y. Cao, K. Wei, G. Min, J. Weng, X. Yang, and Z. Sun, "A Geographic Multicopy Routing Scheme for DTNs With Heterogeneous Mobility," IEEE Systems Journal, 2016.

[16] T. Wang, Y. Cao, Y. Zhou, and P. Li, "A survey on geographic routing protocols in delay/disruption tolerant networks," International Journal of Distributed Sensor Networks, vol. 12, p. 3174670, 2016.

[17] Y. Cao, N. Wang, Z. Sun, and H. Cruickshank, "A reliable and efficient encounter-based routing framework for delay/disruption tolerant networks," IEEE Sensors Journal, vol. 15, pp. 4004-4018, 2015.

[18] A. Basit, S. B. Qaisar, H. R. Syed, and M. Ali, "SDN Orchestration for Next Generation Inter-Networking: A Multipath Forwarding Approach," IEEE Access, 2017.

[19] J. Son, A. V. Dastjerdi, R. Calheiros, and R. Buyya, "SLA-aware and Energy-Efficient Dynamic Overbooking in SDN-based Cloud Data Centers," IEEE Transactions on Sustainable Computing, 2017.

[20] V. G. Nguyen and Y. Kim, "Proposal and evaluation of SDN-based mobile packet core networks," EURASIP Journal on Wireless Communications and Networking, vol. 2015, pp. 1-18, 2015.

[21] J. Wang, Y. Yang, J. Mao, Z. Huang, C. Huang, and W. Xu, "Cnn-rnn: A unified framework for multi-label image classification," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 2285-2294.

[22] T. Zhu, D. Feng, F. Wang, Y. Hua, Q. Shi, Y. Xie, et al., "A Congestion-Aware and Robust Multicast Protocol in SDN-based Data Center Networks," Journal of Network and Computer Applications, 2017.

[23] V.-G. Nguyen, T.-X. Do, and Y. Kim, "SDN and virtualization-based LTE mobile network architectures: A comprehensive survey," Wireless Personal Communications, vol. 86, pp. 1401-1438, 2016.

[24] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on network virtualization hypervisors for software defined networking," IEEE Communications Surveys & Tutorials, vol. 18, pp. 655-685, 2016.

[25] S. Park and Y. Yoo, "Network Intelligence Based on Network State Information for Connected Vehicles Utilizing Fog Computing," Mobile Information Systems, vol. 2017, 2017.

[26] S. Sundar, P. Arora, S. Agrawal, R. Kumar, and H. M. Kittur, "Testing MANET Protocol using Zigbee based Xbee Modules," Indonesian Journal of Electrical Engineering and Computer Science, vol. 3, pp. 441-445, 2016.

[27] J. Garcia-Luna-Aceves, "MANET Protocol Simulations Considered Harmful: The Case for Benchmarking," IEEE Wireless Communications, 2013.

[28] M. Bidaki and M. Masdari, "Reputation-based clustering algorithms in mobile ad hoc networks," International Journal of Advanced Science and Technology, vol. 54, pp. 1-12, 2013.

[29] B. Rashid, M. H. Rehmani, and A. Ahmad, "Broadcasting strategies for cognitive radio networks: taxonomy, issues, and open challenges," Computers & Electrical Engineering, vol. 52, pp. 349-361, 2016.

[30] A. Detti, D. Tassetto, N. B. Melazzi, and F. Fedi, "Exploiting content centric networking to develop topic-based, publish–subscribe MANET systems," Ad hoc networks, vol. 24, pp. 115-133, 2015.

[31] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," 2000.

[32] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," Service assurance with partial and intermittent resources, pp. 239-254, 2004.

Figures

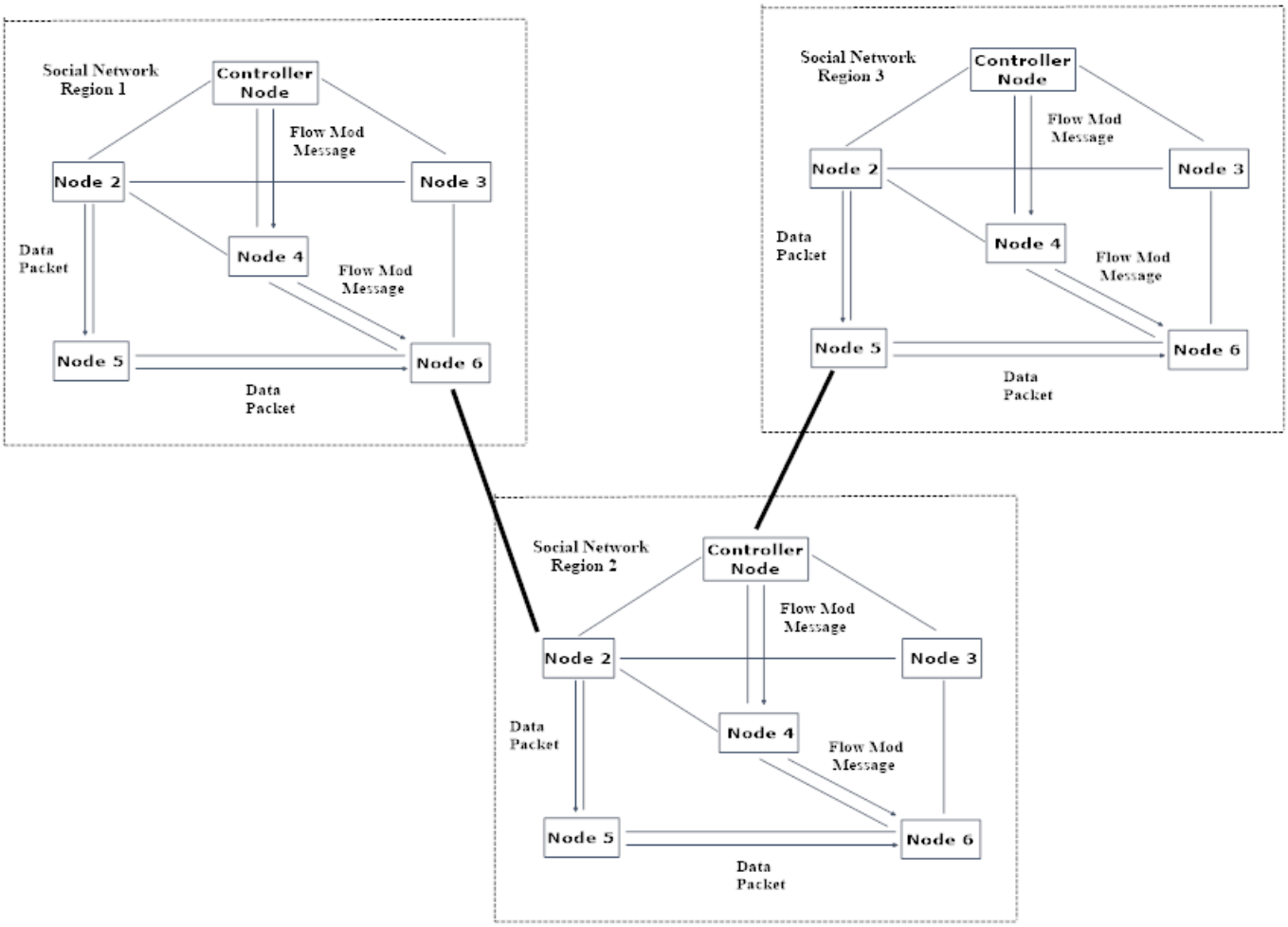

Figure 1

Social Network model based on MANET

Figure 2

Proposed Work Flow.

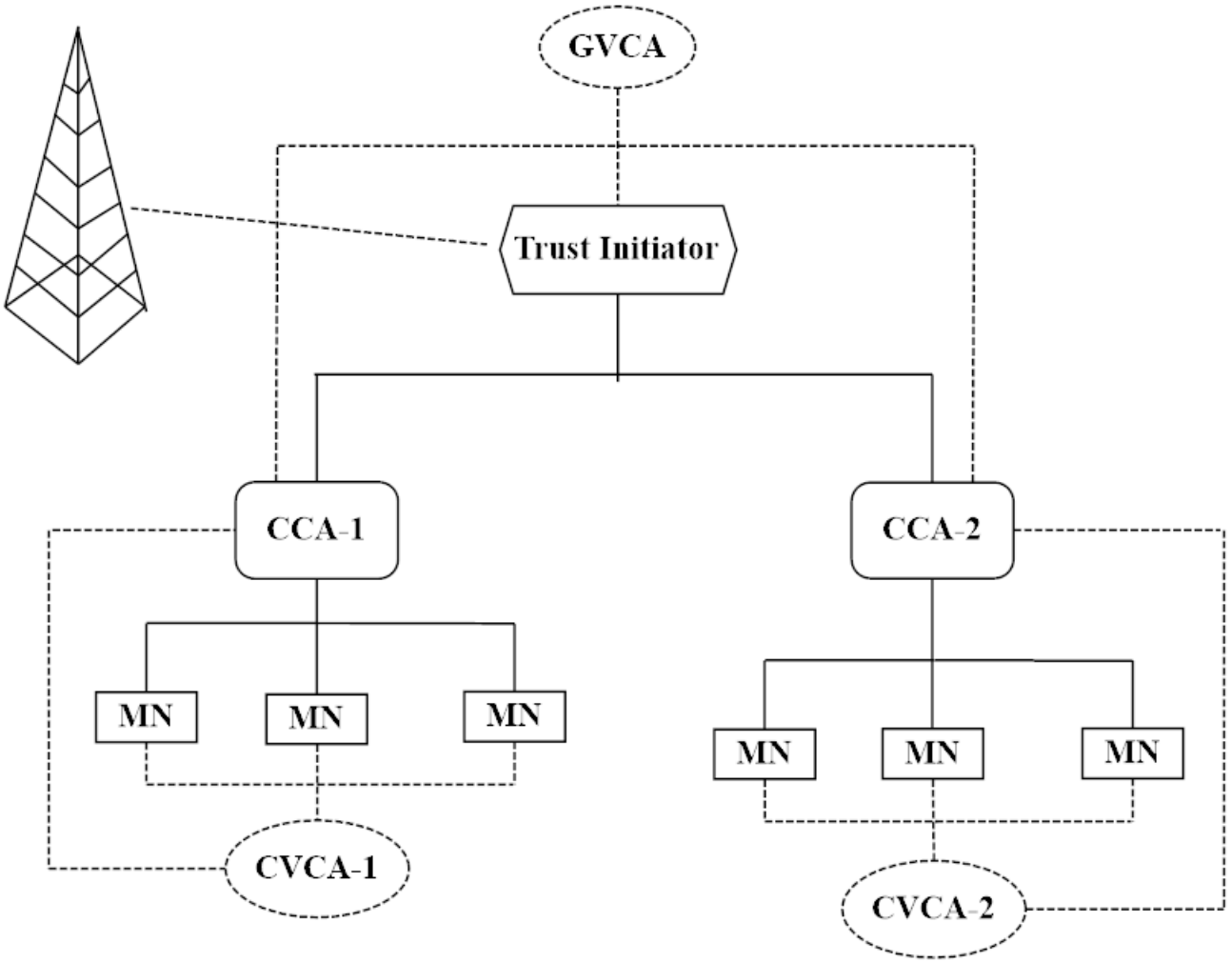

Figure 3

Integration of the VCA infrastructure to MANET

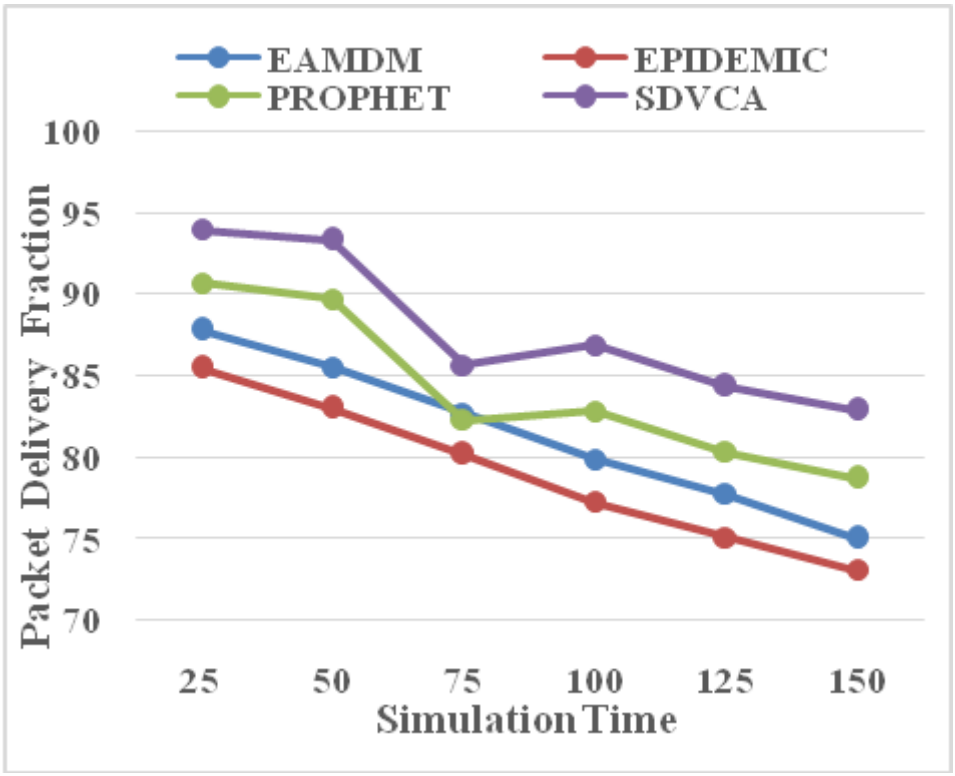

Figure 4

Packet Delivery Fraction vs. Simulation time

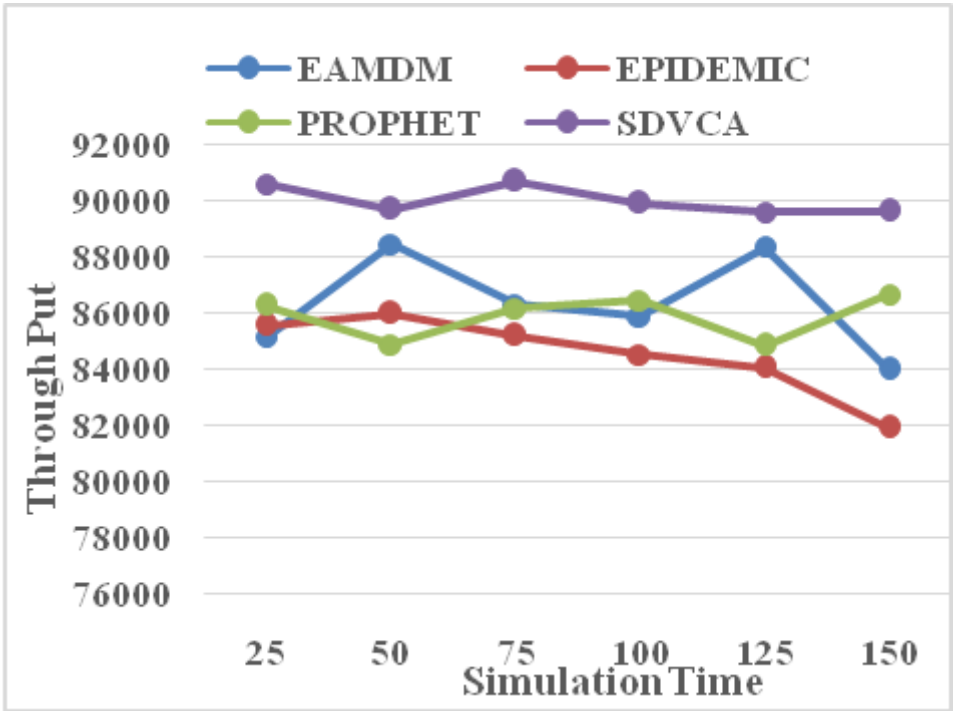

Figure 5

Throughput Vs Simulation

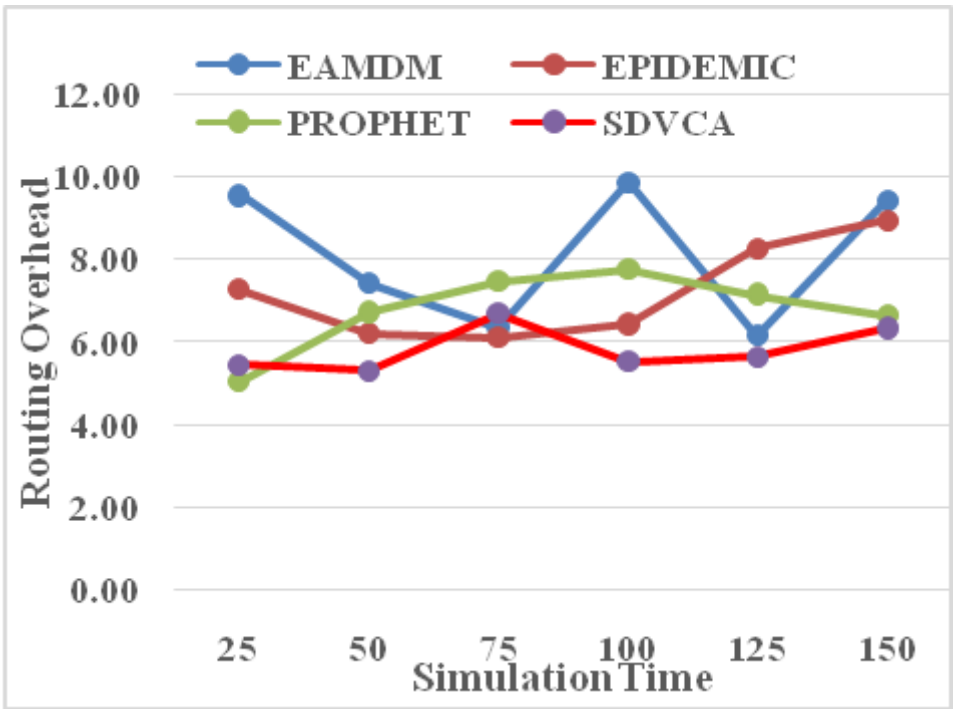

Figure 6

Routing Overhead Vs Simulation time

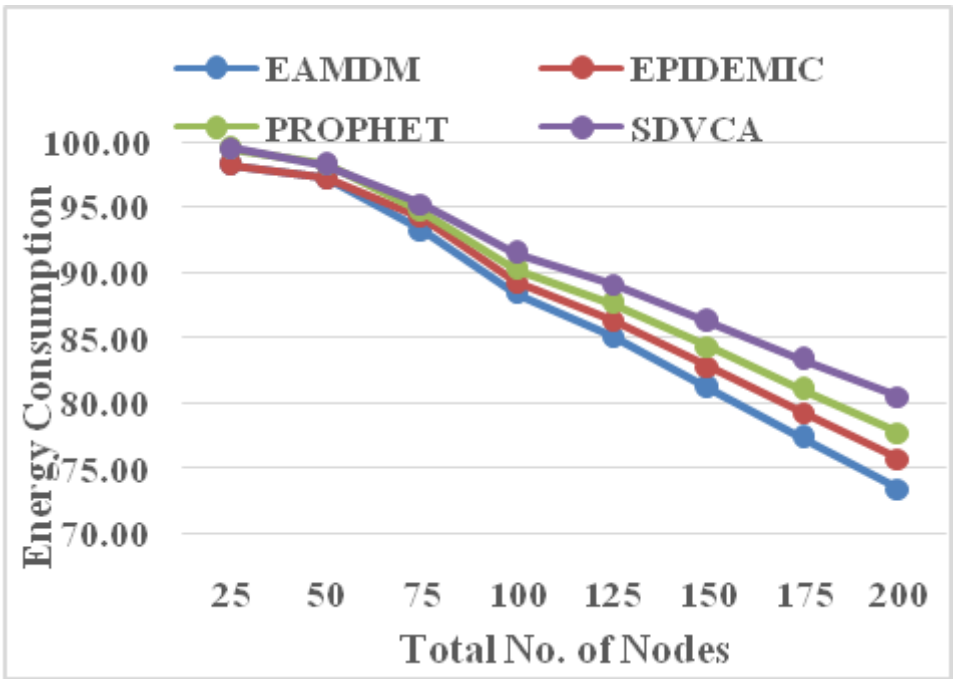

Figure 7

Energy Consumption Vs Total nodes.

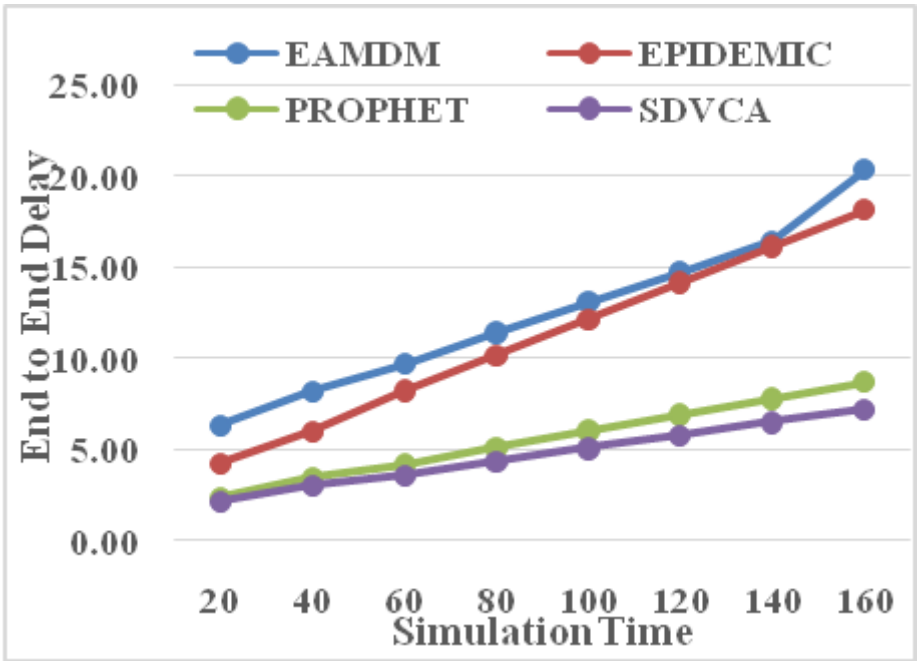

Figure 8

End to End delay Vs Simulation time.