ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 3, Issue 3 (July - Sept. 2016)
International Journal of Advanced Research in Education & Technology (IJARET)

A Novel QKD based DTN in Cloud based Architecture for Military Networks

[I]Akhil V.V., [II]Jisha S.
[I]P.G Scholar, [II]Assistant Professor
[I,II]Dept. of CSE, Mohandas College of Engg. and Technology, Anad, Nedumangad, Kerala, India

Abstract
Mobile nodes in military networks such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity problems. Delay and Disruption-Tolerant Network (DTN) technology is one of the state of the art solutions that allow wireless devices carried by military officers to communicate with each other. DTN technique is used for long area communication in computer network, where there is no direct connection between the sender and receiver and also in the absence of Internet facility. Delay and Disruption tolerant network generally perform store and forward techniques; as a result of which intermediate node may also get access to the message. Aim of this paper is to propose and evaluate quantum key distribution (QKD) technique for enhancing security issues related to DTN. This thesis work also includes a novel communication standard that uses GPS (Global Positioning System) and cloud communication. GPS is for identifying location of remote node in a DTN communication scenario. Since DTN uses store and forward technique, intermediate mobile node gets several messages which drain their energy. Cloud computing is a better solution and through this work, a DTN with cloud computing is implemented and tested. The results show that the proposed solutions are best suiting for DTN.

Keywords
Delay and disruption tolerant network (DTN), global positioning system (GPS)

I. Introduction

Internet is a better medium to communicating different devices in world wide. For transferring of message from one device to other TCP/IP protocol place a major role. TCP/IP protocol works based on certain assumptions, they are

- End to end path between source and destination is exist.
- All the routers and end stations support TCP/IP protocol.
- End point based security mechanism is highly secure.
- Retransmission based on timely and stable form.

For some situation these criteria's may fail, for this purpose introduces a new technology called DTN. DTN is the better solution for following cases.

- If there is no end to end connection between source and destination
- Long propagation delay between the nodes.
- Asymmetric data rate and high error rate etc.

DTN uses store and forward techniques for achieving the above advantages. The store and forward technique specify that whole messages or a piece of messages are moved from a storage node to storage space of another node as shown in Fig. 1. Internet routers use memory chips or internet buffers to store incoming packets. But these techniques have very few millisecond storage capacities. But DTN requires persistent storage because

- A communication link to the next hop may not be available for a long time.
- User within a communicating pair may send or receive data much faster or more reliably than the other node.
- A message, once transmitted, may need to be retransmitted if an error occurs

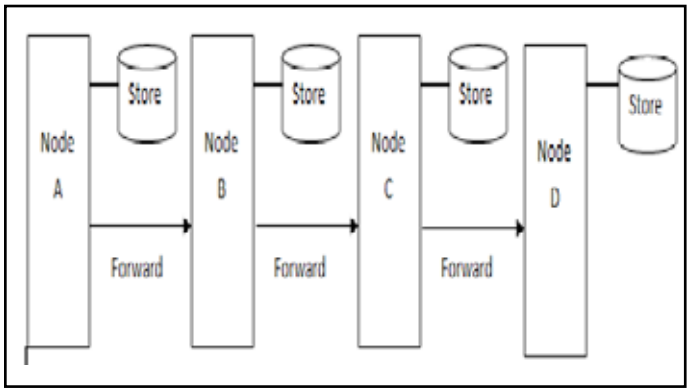

Fig.1: Store and forward technique.

The store and forward technique uses new protocol called bundle protocol. The bundle protocol stores information as bundle and forward to adjacent node. The structure of the bundle protocol is shown in Fig. 2. The bundle layer in DTN protocol helps to communicate application programs to same or different set of lower layer protocols under the condition that long network delays or disruption. The bundle protocol generally contains three things, they are

- Bundle header.
- Source applications user data.
- Optional bundle trailer.

Bundle header contains one or more DTN blocks inserted bundle agent. Source applications user data specifies how to store the data, how to process the data, how to handle the data and how to dispose the data. The optional bundle trailer consisting of zero or more DTN block inserted bundle agent. Now a day's DTN has several applications, DTN is normally used in international space station communication, military and intelligence, commercial purpose like vehicle tracking, agriculture monitoring and underground mining, engineering and scientific research, environmental monitoring,

public service and safety, and personal use.

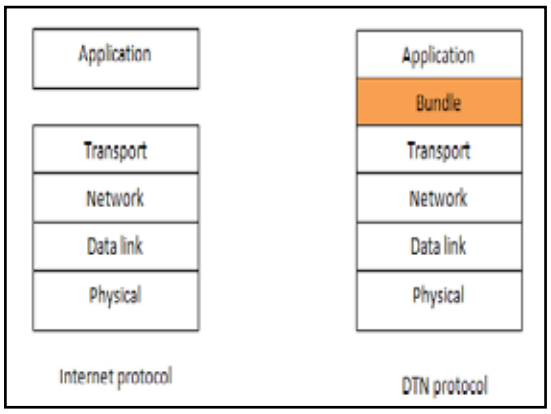

Fig. 2 : Comparison of Internet Protocol and DTN protocol.

The rest of the paper is organized as follows. Section II describes related work. Section II describes the technological back ground. Proposed work is described in section IV. Section V describes result analysis and section VI concludes the paper.

II. Related Work

In the case of DTN techniques there is no direct path from source to destination. DTN techniques are generally use store and forward techniques which pass the information to the nearest node and so on this way destination can get the message [1,2]. To avoid unauthorized access the message should be in the encrypted form. The challenging task is protection of secret keys. Several key transfer algorithms are presented for obtain this.In these types of working a node can get the duplicate of message. Several algorithms are present for obtain the path from source to destination the most suitable one is *Adhoc on demand distant vector routing protocol* (AODV) [3-6]. The figure 3 shows the general architecture of DTN networks and figure 4 shows how DTN work when we use AODV protocol. In the case of fig 3 the node N_1 act as a source and node N_7 act as a destination. The source wants to transfer a piece of information to the destination. The important thing is that there is no direct path from source to destination. Then the node N_1 passes the information to the nearest nodes N_2, N3, and N4. These nodes pass the information to other nodes and so on. The node N_2 andN_5 get multiple messages from multiple sources, and then the duplicate of message should occur as shown in the figure 2.2 [7-10] .

The main problems in implementing DTN technique is that the source node does not know the exact position of destination node. As a result the node cannot predict the time required to reach message at the destination node. One of the important problems is that the architecture contains hundreds of nodes and each node gets several messages but the energy capacity of the nodes is very limited. If the source nodes know the exact position of destination node, the node can choose the easy and accurate way to reach the message to the destination. This time the nodes get only the necessary information and as a result few energy problems can be avoided. This approach yield easy to calculation of the time required for performing the operation. If we use cloud technique at that time the intermediate node gets the necessary information only, using this method energy problem can be avoided completely.

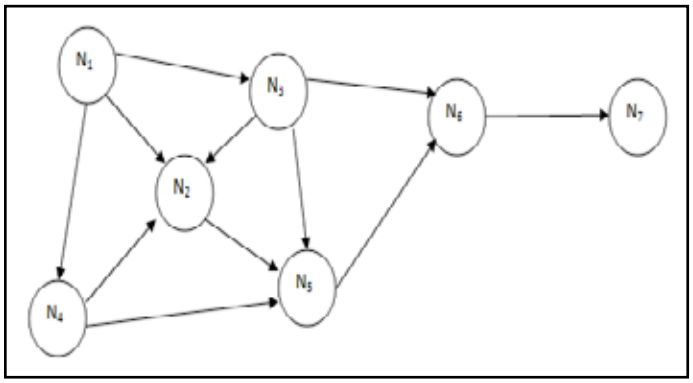

Fig. 3 : General architecture of DTN

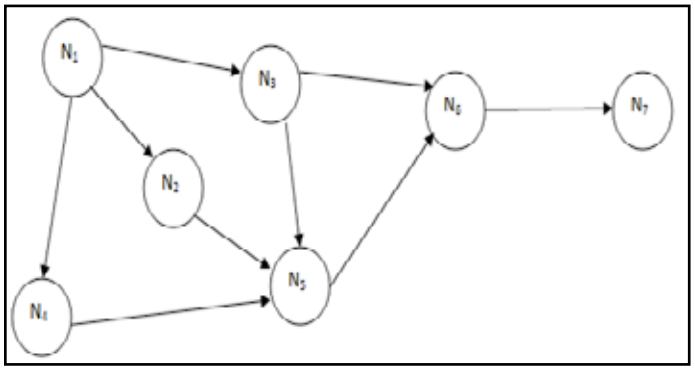

Fig. 4 : General architecture of AODV protocol

III. Technological Background

A. Global Positing System

Positioning, navigation, and timing services are the utilities provided by GPS. The space segment, the control segment, and the user segment are the various segments of GPS. The space segment consists of a nominal constellation of 31 operating satellites that transmit one-way signals that give the current GPS satellite position and time. The Control Segment tracks the GPS satellites, uploads updated navigational data, and maintains health and status of the satellite constellation. The user segment consists of the GPS receiver equipment and uses the transmitted information to calculate the user's three dimensional position and time.

B. Cloud Computing

Cloud computing is a computing style in which scalable and flexible IT functionalities are delivered as a service to external customers using Internet technologies. Cloud computing is not a revolutionary idea; Instead, it is an evolutionary concept that integrates various existing technologies to offer a useful new IT provisioning tool. Cloud applications extend their accessibility through the internet by using large data centers and powerful servers that host web applications and services. Anyone with a suitable Internet connection and a standard Internet browser can access a cloud information and application.

IV. Proposed Work

A. Key transfer mechanism in DTN

General Key exchange can be classified into mainly two they are symmetric key exchange and asymmetric key exchange. In the case of symmetric key exchange same key is used for encryption and decryption. But in the case of asymmetric key exchange technique public key is used for encryption and private key is

used for decryption. In the case of symmetric and asymmetric key exchange technique the key is all ready known. To avoid the previous knowledge introduced another technique is called Diffie-Hellman key exchange technique. In the case of Diffie-Hellman key exchange the sender and receiver used technique is shown in figure.5 and example is shown in figure.6 In the case of Diffie-Hellman key exchange prior knowledge about p and g is needed then only perform these operations. To avoid these problems introduced another techniques is called central authority technique. In the case of central authority techniques central authority is used to provide key for sender and receiver. In this case any damage or compromised it will completely affect the system.fig.7shows the architecture of central key authority.

The most suitable key exchange technique for DTN is quantum key distribution (QKD).Quantum cryptography is not a new algorithm to encrypt and decrypt data. Rather it is a technique of using photons to generate a cryptographic key and transmit it to a receiver using a suitable communication channel. Key plays the most important role in cryptography; it is used to encrypt/ decrypt data. In quantum cryptography, the source sends a key to the receiver, and this key can be used to decrypt any future messages that are to be sent.

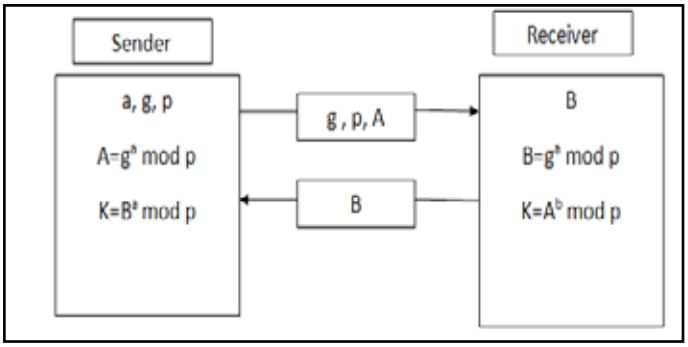

Fig. 5 : Diffie-Hellman method of key exchange.

Sender	Receiver
P =23 g=5	P =23 g=5
a=6	b=16
$A= g^a \bmod p = 5^6 \bmod 23 = 8$	$B= g^b \bmod p = 5^{15} \bmod 23 = 19$
$K= B^a \bmod p = 19^6 \bmod 23 = 2$	$K= A^b \bmod p = 8^{16} \bmod 23 = 2$

Fig. 6 : Example of Diffie-Hellman key exchange

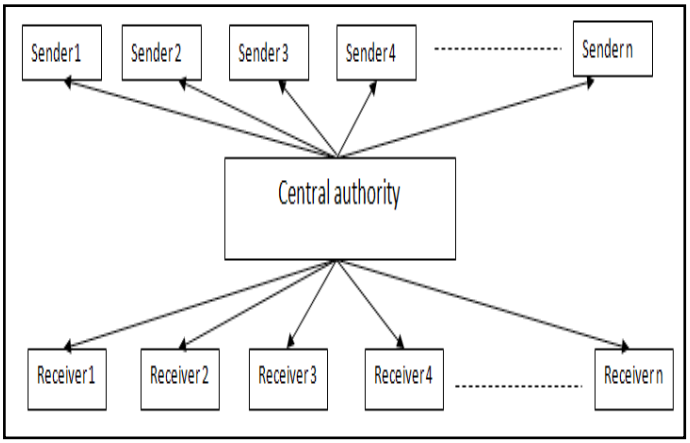

Fig. 7 : Architecture of central key authority

When the key has been successfully sent and received, the next step is to send encrypted data to the receiver and let it decrypt and process that data. Quantum cryptography is working based on Heisenberg uncertainty principle. Heisenberg uncertainty principle states that it is impossible to find simultaneously both the position and momentum of a microscopically moving particle. Normally quantum cryptography uses spins of photons. Photon means smallest particle of light. Photons contains four types of spin they are

- Horizontal spin (-)
- Vertical spin (|)
- Left diagonal spin (/)
- Right diagonal spin (\)

Photons have the capability of spin four types at the same time. several algorithms are presented in quantum cryptography most widely used is BB84 algorithm which is proposed by Bennet and Bassard in 1984.in the case of BB84 algorithm two band pass filters(bases) are used they '+'band pass filter and '**X**' band pass filter as shown in fig 8.

Band pass filter	Output spin	
'+' band pass filter	Horizontal spin(-)	vertical spin(|)
'X' band pass filter	Left diagonal spin(\)	Right diagonal spin(/)

Fig. 8 : General spin of BB84 algorithm

In the case of BB84 algorithm data is associate with photon is associate with assign 0 and 1. Normally '+'band pass filter passes horizontal and vertical spins, '**X**' band pass filter passes left diagonal and right diagonal spins as shown in fig 9.

Spin	Horizontal(-)	Vertical(|)	Left diagonal(\)	Right diagonal(/)
Value	0	1	0	1

Fig 9 general working of BB84 algorithm

Quantum key distribution starts with Alice sending some key to Bob. The important thing is that Alice and Bob contains a special equipment for obtain the keys. The communication is obtained through the free space or optical fibers. Each photon can carry one bit of information. Alice can choose appropriate bases for sending the information. On the receiver side Bob chooses bases according to her convenience should not specified any information about the bases. Sometimes Alice and Bob will randomly choose the same bases, at that time they will get the same value for the photon which is useful. When Alice and Bob measure the photon using different bases, then the error exist and should not get the final answer. After perform the decryption do not get the meaningful message Alice and Bob publically speak about which bases is used for obtain this Bob send to Alice. Alice sends the reply and reconstructs it. Two important reasons this technique is highly secure, first one is Alice and Bob got the received message they perform the operation and discarded it. The second thing is Alice and Bob do not disclose the final measurement key and results. The illustration of QKD operations is shown in figure 10.

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

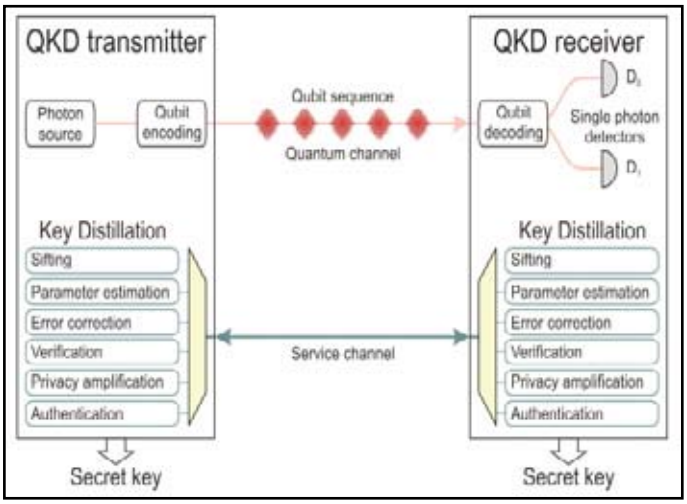

Fig. 10 : illustration of QKD operation.

B. Location identification of mobile nodes

One of the most suitable solutions to avoid the above said problems is using GPS technology. GPS module deals with position based services. Using this module, user can find his/her own position, friend position and family member position. Using the GPS technology we can easily identify the location of remote node. The major advantage of using GPS technology is that it works without internet. All the nodes contains the GPS facility which can easily identify the location and nearest node to reach the destination node [11] [12]. The fig.11 shows the architecture of GPS technology working in DTN. Suppose node N_1 wants to transfer a piece of information to node N_7. Using GPS technology node N_1 identifies the location of node N_7. Then it chooses easy path to reach the destination node and transfer the message to adjacent node which is present nearest. The node N_3 get the message and the node know the destination then using the GPS technology it identifies the easiest path from source to destination and pass the information to the nearest node. All the nodes repeat the process because the nodes are mobile. Finally the destination node gets the result. As a result time and bulk of message transfer in intermediate node can avoid.

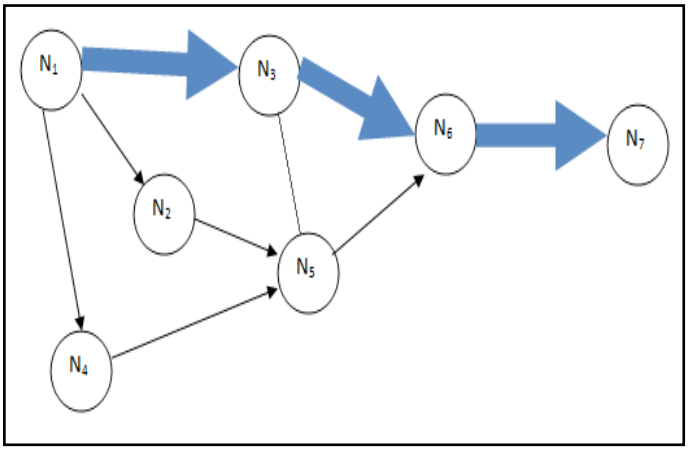

Fig. 11 : GPS technology working in DTN

C. Energy saving method of mobile node

The most suitable and accurate energy saving method in DTN is using cloud technique. If we use cloud technique we can encrypt the message and passing the message to the cloud. The packet format specifies the source, destination sequence and other details. Using GPS technique we know the exact location of mobile remote node and nearest mobile node which is in the range. It informs the nearest node using easy path method. The information packet contains a time to live block and it destroy after particular time. The remote node get the message it passes an acknowledgement message to the sender through the method explained above. Using this method 20% of energy of mobile node is saving.

V. Result Analysis

For obtain the result analysis we simulate the system in network simulator second (NS2). We implement the system with 20 mobile nodes and calculate the time required to complete the message transfer using GPS and without using GPS. Ns2 should not support the GPS module, for obtain this we can implement the system with accessing the coordinate values and calculate the distance with Euclidian formulae. the Euclidian formulae shown in equation (1).

Distance $d= (x_2-x_1)^2-(y_2.y_1)^2$ (1)

Fig 12 shows that the time required for communication using GPS and without using GPS. Also we have conducted experiment for analyzing the number of packets received by each node for different simulation time. Our experimental results are plotted in Fig 13 where time of simulation is represented along X-axis and Number of packets exchanged along Y-axis. Then we calculate the energy of a mobile node with varying time, using same scenario using cloud and without using cloud with the help of green cloud module. The experimental result is shown in fig 14 where time on the x-axis and remaining energy on the Y-axis.

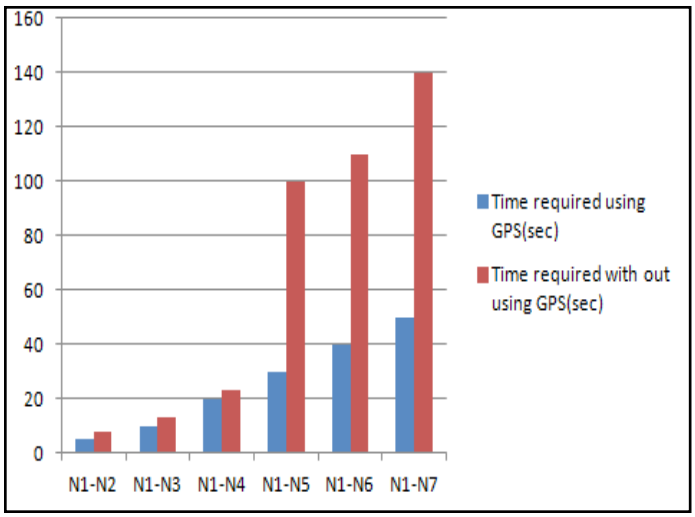

Fig 12 Time analysis- communication using GPS and without using GPS

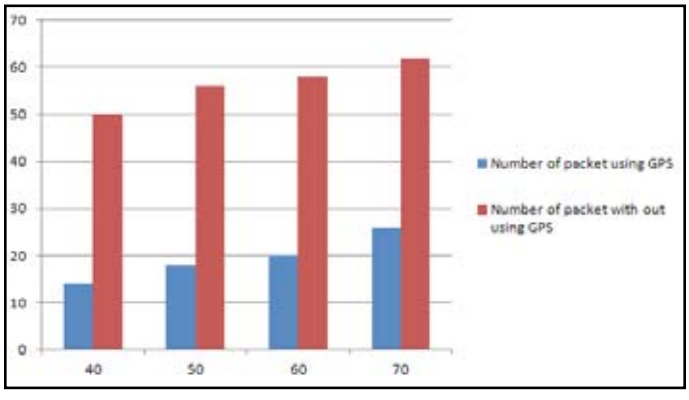

Fig. 13 : Number of packets exchanged for different simulation time period

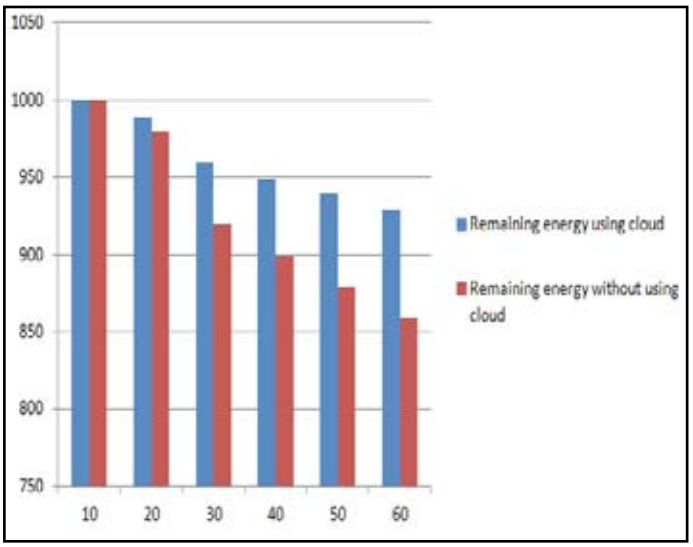

Fig. 14 : Remaining energy comparison using cloud and without using cloud.

VI. Conclusion

DTN technologies are suitable for long area communication in computer network, where there is no direct connection between the sender and receiver and also in the absence of Internet facility. The main problems in implementing DTN technique is that due to node mobility, source node does not know the exact position of destination node. Since store and forward technique is used, number of packet exchanged among the nodes is also very high. This leads to several resource utilization problems. Through this paper we have proposed and illustrated an effective approach that can be used with DTN. Using this method time and energy needs of communication can reduce. The main application is focused on military area.

Reference

[1] *Akhil V.V., Jisha S., "Survey on Encryption Techniques in Delay and Disruption Tolerant Network International Journal of Advanced Engineering, Management and Science (IJAEMS) [Vol-2, Issue-1, Jan- 2016].*

[2] *Sonika Gandhi, A.N. Jaiswal,, "A Method forDetecting Attacks on Delay Tolerant Network," International Journal of Advanced Computational Engineering and Networking, Volume-2, Issue-6, June-2014.*

[3] *Sarawagya Singh, Elayaraja.K, "A survey of misbehaviors of node and routing attack in delay tolerant network," International Journal of Science, Engineering and Technology Research, Volume 4, Issue 2, February 2015.*

[4] *P. Eronen, Ed.Nokia, "DES and IDEA Cipher Suites for Transport Layer Security (TLS)," RFC 5469, February 2009.*

[5] *JH. Song, R. Poovendran, "The AES-CMAC Algorithm," RFC 4493, June 2006.*

[6] *Frank Nordemann, Ralf Tönjes ,"Transparent and autonomous store-carry-forward communication in Delay Tolerant Networks (DTNs)," Specifications Version 2.1", RFC 3447, February 2003.*

[7] *Biren Patel , Dr. Vijay Chavda, "DES Comparative Study of DTN Routing Protocols," RFC 5469, February 2012.*

[8] *Nilam Chaudhary , Prof. Shakti Patel, "A Survey on Routing Protocols in Delay-Tolerant Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015.*

[9] *Nitiket N Mhala and N K Choudhari , "An Implementation Possibilities For Aodv Routing Protocol In Real World" International Journal of Distributed and Parallel Systems (IJDPS) Vol.1, No.2, November 2010.*

[10] *Sheng Liu, Yang Yang, Weixing Wang,"An Research of AODV Routing Protocol for Ad Hoc Networks" 2013 AASRI Conference on Parallel and Distributed Computing and Systems.*

[11] *Pankaj Verma, J.S Bhatia, "Design And Development Of Gps-Gsm Based Tracking System With Google Map Based Monitoring" International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, No.3, June 2013.*

[12] *Mahesh Kadibagil, . H S Guruprasad, "Position Detection and Tracking System" International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 4, No. 3, June 2014.*

.