A Comparison analysis of Tolerant Networks schemes

W. Melba Marries[1] S. Christal Anand[2]

Department of Computer Science, Scott Christian College, Nagercoil
Assistant Professor, Lord Jegannath College of Engineering and Technology, Nagercoil

Abstract—Many applications are based upon a military network communications model, i.e., they require packet delivery from one or more authorized senders and authorized receivers. i.e., providing confidentiality, integrity, and authenticity of messages delivered between network groups of members will become a critical networking issue. The Disruption tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by node (member) to communicate with each other and access the confidential information. In this paper, we show comparative analysis of different Tolerant Networks schemes which is useful for researchers/Authors/readers to know about the Different Tolerant Networks.

Keywords—Access control, Distributed Network, Encryption, Decryption, Multi authority, Secure data retrieval, Network application

I. INTRODUCTION

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. [1][12]

However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.[1]

Novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, we propose cryptographic optimizations that vastly improve enforcement efficiency. Attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. [1][4][12]

Traditional ad hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. Hence, routing mechanisms that can withstand disruptions need to be designed. A store-and-forward approach has been proposed for delivering messages in disruption tolerant networks. Recently, several approaches have been

proposed fornicate routing in disruption-prone networks e.g. the 2-hop relay approach, delivery probability based routing, and message ferrying schemes. In our earlier paper, we have evaluated a combined multi hop and message ferrying approach in disruption tolerant networks. Special node is designated to be a message ferry. A more flexible approach is to let regular nodes volunteer to be message ferries when network dynamics mandate the presence of such ferries to ensure communications. Thus, node-density based adaptive routing (NDBAR) scheme that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communications. Our simulation results indicate that our NDBAR scheme can achieve the highest delivery ratio (compared to other DTN routing approaches) in very sparse ad hoc networks that are prone to frequent disruptions. [3][12]

Our Contributions: In this paper shows comparison of different scheme for Disrupted tolerant networks. The Disruption tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by node (member) to communicate with each other and access the confidential information.

II. DISRUPTION TOLERANT NETWORKS

A. Context-Aware Multicast Routing Scheme

Disruption Tolerant Networks (DTNs) are emerging solutions to networks that experience frequent network partitions and large end-to-end delays. Several schemes have been proposed for multicast routing in DTNs assuming the availability of different amounts of knowledge about network topology, etc. Context aware adaptive multicast routing (CAMR) schemes better for DTN. The CAMR (Context aware multicast routing scheme) scheme can achieve the highest message delivery ratio, with similar delay performance especially when the nodes are very sparsely connected. We also perform sensitivity analysis on the tunable parameters of our CAMR scheme and evaluate the delivery performance of CAMR in different scenarios e.g. different number of groups, different maximum node speeds. Our results indicate that CAMR scales well and provides excellent delivery performance in many different scenarios. [11][12]

(a) Local Node Density Estimation

Each node periodically (e.g. every 20 ms) broadcasts a neighbor discovery packet using regular power transmission. [9][11] On receiving a neighbor discovery packet, a node composes a neighbor response packet including this node's information and this node's 1-hop neighbor's information and sends the neighbor response packet to the originator of the neighbor discovery packet after some random back off delay. [9][11][12] Thus, each node can estimate the number of neighbors it has periodically, denoted as N. If a node's N drops below a threshold K, during a neighbor discovery period, the node sets a sparsely connected flag.

(b) 2-hop Neighbor Contact Estimation

Each node also maintains its contact probabilities with its 2-hop neighbors. [9][11] The contact probability of a neighbor is set to 1 as long as a node, ni, can receive neighbor response messages from a neighbor, nj, periodically. When ni fails to hear a neighbor response message from nj, then ni decreases its contact probability with nj by a factor of β periodically (since the neighbor discovery message is sent out periodically). Rather than immediately reducing the contact probability to zero, the aging factor, β, is used to avoid the ping-pong effect (i.e. a node may move in and out of the transmission range frequently). These contact probabilities allow a node to send the messages directly without incurring the route discovery overhead if the destination happens to be within its 2-hop neighborhood.[11][12]

B. Network Model

A DTN is an overlay network that is built upon underlying networks e.g. wireless ad hoc networks. [5] Its network architecture is based on the asynchronous message (called bundle) forwarding only those nodes that implement the DTN functionalities e.g. sending, storing, and receiving bundles are considered DTN nodes, while the others are denoted as normal nodes.[5][8] A DTN link may span several underlying links.

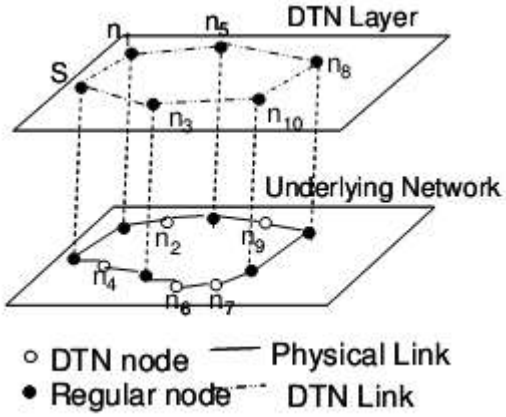

Figure: 1. A Simple DTN Example [11]

C. Multicasting Model

Multicast in DTNs is defined as the one-to-many or many-to-many bundle transmissions among a group of DTN nodes. A multicast source uses either a multicast end-point identifier descriptor (EID) e.g. *.cse.lehigh.edu, or an explicit list of the names of individual DTN multicast receivers as the destination address for multicast bundles. The later approach may not be scalable when the number of DTN multicast receivers grow large. [9][11][12]

D. Dynamic tree-based multicasting algorithm

This is a dynamic tree-based multicasting algorithm designed for DTNs. In DTBR, the upstream node will assign the receiver list for its downstream neighbors based on its local view of the network conditions. [11]The downstream nodes are required to forward bundles only to the receivers in the list, even if a new path to another receiver (not in the list) is discovered. For example, in Figure 2(a), let say link 1-2 is unavailable when the multicast bundle reaches node 1. Then, node 1 will use node 3 to deliver to nodes 5 and 6 and store a copy of the bundle.[10][12] Node 1 can send the stored bundle to node 2 when the link 1-2 becomes available again since this is the only route (via link 1-2) that node 1 knows of to reach node 4. DTBR assumes that each node has complete knowledge or the summary of the DTN link states in the network.[11][12]

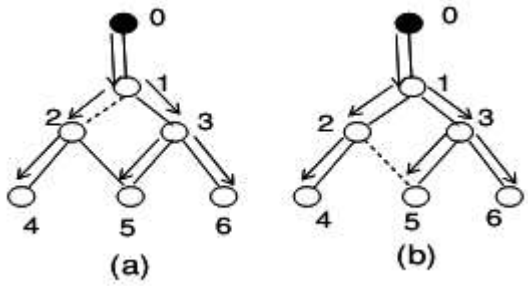

Figure. 2. Multicast approaches in DTN (a) DTBR, (b) OS-multicast: when link 25 is unavailable and link 3 to 5 becomes available, node 3 will take advantage of the current available link immediately [11]

E. On-demand Situation-aware multicast

A unique multicast tree is constructed for each bundle and the tree is adjusted at each intermediate DTN node according to the current network conditions. [9][11] When a DTN node receives a bundle, it will dynamically adjust an initially constructed tree based on its current knowledge of the network conditions. [11][12] Via such adjustments, any newly discovered path will be quickly utilized.

III. Delay Tolerant Networks

A. Anonymous networking in delay tolerant networks

ARDEN (Anonymous networking in delay tolerant networks), an anonymous communication mechanism for DTNs based on a modified onion routing architecture. Instead of selecting specific nodes through which messages must pass as is traditionally done in onion

routing, ARDEN uses Attribute-Based Encryption (ABE) to specify and manage groups that may decrypt and forward messages. In this approach not only increases throughput and reduces end-to-end latency over traditional onion routing techniques, but also adds minimal overhead when compared to DTN routing protocols that do not provide anonymity guarantees. Through this, we show that ARDEN is an effective solution for anonymous communication in intermittently connected networks such as DTNs. [4][9][10][12]

The following contributions:

- Design a robust anonymous communication protocol for DTNs: We develop ARDEN, an anonymous networking protocol for DTNs. ARDEN builds on a traditional onion routing architecture but incorporate Attribute-Based Encryption (ABE) to simplify management and drastically reduce latency while providing strong anonymity guarantees [9][10][12]

B. DTN network model

A DTN is composed of a set of nodes. The period of time when two nodes are within direct communication range is called contact. Within a contact, nodes can transfer bundles (i.e., DTN packets) to each other. [9]The duration and transfer bandwidth of a contact is limited. A node can deliver bundles to a destination node directly if within radio range or otherwise via intermediate nodes. Nodes have a limited buffer space to temporarily store the in-transit bundles. When a node's buffer is full, it will drop bundles. Destination nodes are assumed to have enough storage for delivered bundles. Finally, we assume that a node is able to obtain the IDs of a large proportion of nodes in the DTN, which is essential to onion routing and its variations. It can be achieved by periodically disseminating node information [9][10][12]

C. Application

The DTN concept was initially de-signed for communicating with spacecraft, to compensate for disconnections over interplanetary distances. However, over the years, researchers have identified numerous terrestrial environments where DTN concepts may be employed.[10] Example - Underwater networks make use of the DTN paradigm to enable applications for oceanographic data collection, pollution monitoring, offshore exploration, disaster prevention, assisted navigation and tactical surveillance applications [10]. Wildlife tracking networks, which are designed for biology research, allow monitoring the long-term behaviour of wild animals sparsely distributed over a large area. [9][10][12]

D. ARDEN design

The goal of ARDEN is to provide an efficient anonymous communication mechanism for DTNs. To achieve this, ARDEN builds upon a foundation of onion routing and modifies it for disconnected environments. The lack of long-lived paths between contacts makes the single path of onion routing susceptible to performance degradation in DTNs. Further, the complete knowledge of the exact path is hard to obtain in advance. ARDEN overcomes these issues by replacing single-node proxies with groups and through the use of multicast. Every node of a group can decrypt the corresponding layer of the wrapped bundle while only the intended destination can ultimately recover the final encrypted message. Through the communication redundancy provided by multicast, ARDEN manages to find varying latency and loss properties. [9][10][12]

E. Group partitioning and management

ARDEN relies on the presence of groups capable of decrypting and forwarding traffic to its receiver. In order for this approach to work, it is necessary to divide nodes into groups. We rely on dynamic group partitioning, as it allows senders to specify groups as they see fit and prevents an adversary from necessarily learning group membership. [2][8][9][11][12]

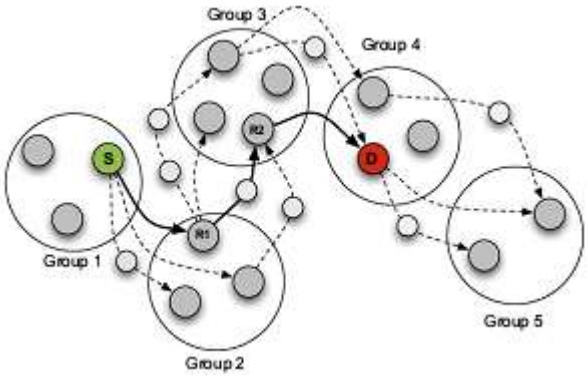

Figure: 3 show, An ARDEN relay path from S to D consisting of multiple forwarding paths, among which the bold path is the shortest. Note that every relay hop may consist of several intermediate nodes. The shortest anonymous relay path is not necessarily the shortest path from S to D. [9]

IV. VEHICULAR DELAY TOLERANT NETWORKS

Vehicular Ad hoc Networks (VANETs) have been an important research topic for many years. It is an extension of Mobile Ad hoc Networks (MANETs) to vehicle systems, spanning to planes, trains, boats, automobiles and robots. [10] Vehicular Ad – Hoc Networks one of the most advanced and efficient networks. VANETs offer various service and benefits to users. In VANETs provide communication between vehicle to vehicle and vehicle to Infrastructure, i.e. between RSU and OBU. This communication needs to be secure and efficiency for vehicular users. Because of attacking and misusing such network could cause serious consequence. [5]

A. MANETs have a set of attributes and requirements[5][8][10]

Self-organization: A MANET does not depend on a pre-existing infrastructure but, rather creates one within the wire-less network itself; the nodes are both router and terminal;
Mobility: Nodes move and protocols have to adapt to this;
Multi hopping: certain nodes can be reached only by hopping over other nodes;
Energy conservation: nodes are typically small devices with a limited power supply;
Scalability: applications can grow at any moment, increasing complexity;
Security: due to their wireless nature, security is complex and a major issue.

B. VANETs have special characteristics

Predictable mobility: Movements are not random, since vehicles have to stay on the road. [10]
High mobility: the network topology changes rapidly because of vehicle speed; [10]
Variable topology in time and place: the network topology evolves depending on time (e.g., traffic jams) and location (urban, rural); [10]
Large scale: all vehicles are potential nodes;
Partitioned networks: the hop range in a wireless car-to-car network is about 1000 m, limiting the communication range of vehicles; [8][10]
No significant power of computation constraints: a vehicle can generate sufficient power. An exception is for stationary nodes, which may be battery operated. [8][10]

C. The main difference between VANETs and VDTNs

VANETs assume that end-to-end connectivity exists through some path, while VDTNs do not [5][8][10]. So, VANETs concepts are more appropriate for dense networks, while VDTNs accept also sparse networks through its store-carry-forward paradigm. VDTNs extend VANETs with DTN capabilities to support long disruptions in network connectivity. The DTN concepts are useful as vehicular networks are characterized by scarce transmission opportunities and intermittent connectivity, particularly in rural or mountainous areas. [10]

D. VDTN Projects and Applications

The **Kiosk Net project** [10] provides low-cost Internet kiosks in rural areas with some services, such as email, web browsing, telemedicine, crop prices information and taxpaying. As the kiosks have no permanent Internet connection, a bus and DTN protocols offer the gateway between the kiosks and the Internet at a neighbouring town.

VDTN (Vehicular-Delay Tolerant Networks) **project** [10] proposes a layered architecture for VDTNs, where the bundle layer is placed below the network layer instead of above the transport layer. The objective is to route large size messages instead of small size IP packets. These results in fewer packet processing and routing decisions, which can result into less complexity, lower cost and energy savings. [10] The architecture uses out-of-band signalling, based on the separation of the control plane and data plane.

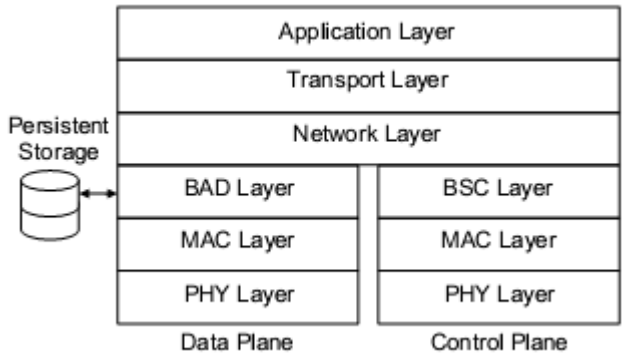

Figure: 4. IP-over-VDTN layered architecture.

CarTel Project [10] offers two DTN networking abstractions: dPipe and CafNet ("carry and forward network"). **DPipe** is a conceptual extension to the UNIX pipe abstraction that allows processes on separate hosts to communicate via a reliable, delay-tolerant data stream. It is implemented using several file based buffers for storage, and, when connectivity is present, uses TCP sockets to send buffered data and application-level acknowledgments to ensure that all data gets written to disk.[10] **CafNet** is a delay-tolerant network stack, which delivers data in intermittently connected environments possibly through mule nodes. [10] The Mule Adaptation Layer hides details of the communication medium from the higher layers. Unlike the traditional sockets interface, the CafNet interface uses call backs across all its layers. By issuing call backs whenever network conditions change, CafNet makes it possible for the sender application to dynamically prioritize data. [10] At the same time, CafNet's network layer provides some buffering to achieve high utilization when network connectivity is fleeting (e.g., a few seconds), a common situation at vehicular speeds.

EMMA Project the Environmental Monitoring in Metropolitan Areas (EMMA) project [56] uses a public bus transportation network to monitor pollution. The buses have a GPS and a number of pollution detection sensors that continuously monitor the environment. The collected data is transmitted through a DTN stack to a central server where it is analysed.

Drive-Thru Internet Project the Drive-Thru Internet project [10] aims to provide Inter-net access for vehicles, by exploiting intermittent connectivity to wireless access points along the road. The concept of Performance Enhancing Proxies (PEP) [10] is used to hide the effects of intermittent connectivity.

CONDOR Project Military communication systems have to adapt to situations that offer several challenges: lack of fixed infrastructure, limited spectrum availability, difficult propagation environments, and rapidly fluctuating information demands by end users. [10]

Non-DTN Projects Although not currently using DTN protocols, a few projects are worth referencing due to their relevance in vehicular networks, either because of their standardization effort or the availability of commercial services. A more complete list can be found in [10].

V. MOBILE DELAY TOLERANT NETWORKS

Introduce our MDTN software by outlining the entities taking part in the system. Initially we extend the general case scenario where software could be operable and then we proceed by reviewing the implemented

scenario. We also show some implementation details along with a real usage case are shown. [12]

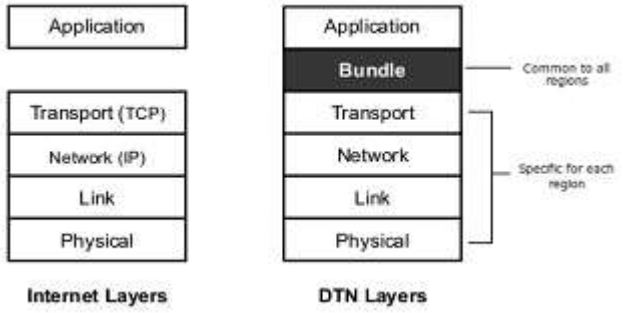

Figure: 5. H DTNs Bundle Layer

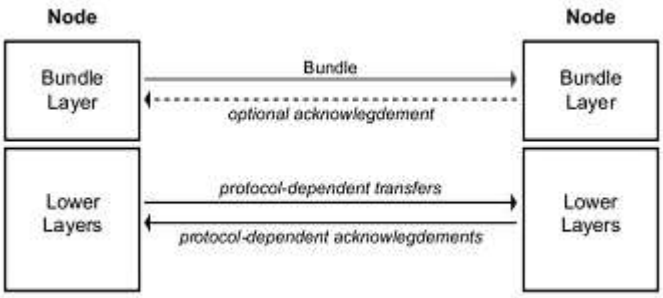

Figure: 6. H DTNs Bundle Protocol stack

A. *MDTN protocol*

The MDTN-client can be in the following two possible states: [12]

Online: when he is connected to the MDTN server;
Offline: when he is disconnected from the service.

MDTN server can be in the following two operating modes: [12]

gathering: server does not have Internet connectivity but he is actively receiving and storing user requests eventually forwarding them stored information previously accomplished for other users that requested them;

Digesting: server reaches Internet connectivity and is able to accomplish (digest) pending user requests (gathering mode is still available).

Both these entities need to implement and use the same communication protocol which is a slightly modified version of the Bundle Protocol. [12] Also, inside a DTN every node that is able to send and receive bundles is called bundle node, which is characterized by the presence of three fundamental components:

- BPA (BP-Application Layer):[12] is the Bundle Layer services supplier, which allows higher levels to communicate through the DTN;
- CLA (Convergence Layer Adapter): [12] is the adapter which allows the Bundle Overlay to be placed over various physical networks that can work with different Transport Protocols (like TCP). There can be more than one adapter for each node;
- AA (Application Agent): [12] is the component that uses the BPA for communications purpose.

B. *MDTN Implementation*

Our MDTN is a Java based application built for Android capable devices and tested on HTC Hero, HTC Desire etc.... It consists of a package composed by a client and a server both sharing the same core module handling the DTN communication.[12] The client consists of a tabbed interface allowing the user to manage and easily interact with the MDTN services. These services are:

1. MDTN-Status: handle service connection and logs;
2. MDTN-Email: send e-mail;
3. MDTN-Files: require and download Internet resources (e.g. web page, multimedia document).[12]

At this point we show by means of an experiment a concrete usage of MDTN. The map in Fig. 9 shows the interactions taking place between the carrier and the user respectively operating MDTN-server and client. In this demo the carrier is a car with a predetermined route and an on board Wi-Fi AP while the user is mobile and operating MDTN-client on an Android enabled device.

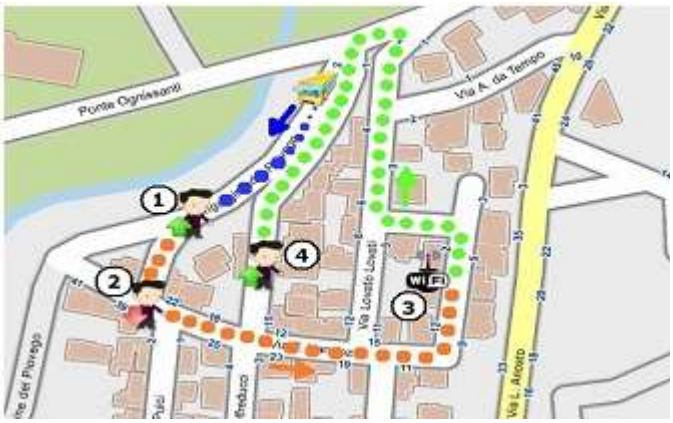

Figure: 7. H Demo map showing the interactions along the route between carrier and user. The blue dots represent the car route with no pending tasks. The orange dots represent the carrier route where there are pending tasks, issued by the user at 2. Along the green dots path the carrier has satisfied user requests (at 3) and is ready to forward the output when user gets on board at 4.

The enumerated points in the map represent the following actions: [12]

1. The user gets on the car and successively forwards MDTN-server a task;
2. The user gets off the car and continues his journey;
3. The carrier is nearby a wireless AP connected to the Internet (e.g. bus station), satisfies users pending tasks and stores the output locally;
4. The user gets on the car and once connected to the MDTN-server retrieves the required content.

VI. CONCLUSION

This Comparison analysis of Tolerant Networks schemes shows that different applications are based upon a tolerant network communications model, i.e., they require packet delivery from one or more authorized senders and authorized receivers. i.e., providing confidentiality, integrity, and authenticity of messages delivered between network groups of members will become a critical networking issue. Based on our comparison analysis the Disruption tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by node (member) to communicate with each other and access the confidential information. We expose different methods and technology of different Tolerant Networks schemes which is useful for researchers/Authors/readers to know about the Different Tolerant Networks.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang, *Member, IEEE, ACM,* "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE/ACM transactions on networking, vol. 22, no. 1, February 2014

[2] Chung Kei Wong Mohamed Gouda Simon S. Lam, "Secure Group Communications Using Key Graphs" Department of Computer Sciences, University of Texas at Austin, Austin, TX 78712-1188

[3] Mooi-Choo Chuah and Peng Yang, "Performance Evaluation of Node Density-Based Adaptive Routing Scheme for Disruption Tolerant Networks"Department of C SE, Lehigh University, USA, Int. J. of Ad Hoc and Ubiquitous Computing, 2006

[4] Matthew Pirretti , Patrick Traynor, and Patrick McDaniel, "Secure Attribute Based Systems" SIIS Laboratory, CSE, Pennsylvania State University, 2006.

[5] F. Sammy and S. Christal Anand, "A Survey of Security in Vehicle to Vehicle communications", ERES Int. Journal of Computer Networks, vol. 1, no 2, 2014

[6] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar, "Identity-based Encryption with Efficient Revocation" Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008.

[7] R. Granger, D. Page, and N.P. Smart, "High Security Pairing-Based Cryptography Revisited" Dept. Computer Science, Woodland Road, Bristol, BS8 1UB, United Kingdom, 2002.

[8] S. Christal Anand and Sumitha, "A Key Management Scheme for VANET based on the Vector group" CIIT Int. Journal of communication, 2011

[9] Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa H. Ammar, Ellen W. Zegura, "ARDEN: Anonymous networking in delay tolerant networks", College of Computing, Georgia Institute of Technology, Atlanta, GA 30332, United States, December 2011

[10] Paulo Rog´erio Pereira, Joel J. P. C. Rodrigues, Joan Triay, "From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks", Member, IEEE, July 2011.

[11] P. Yang, M. Chuah, Context-Aware Multicast Routing Scheme for Disruption Tolerant Networks, CSE Department.

[12] "MDTN: Mobile Delay/Disruption Tolerant Network", C. E. Palazzi, A. Bujari, S. Bonetta, Department of Pure and Applied Mathematics University of Padua, Padua H Italy, G. Marfia, M. Roccetti, A. Amoroso, Deparment of Computer Science, University of Bologna, Bologna H Italy