International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 4, July-Aug-2018, ISSN (Online): 2395-566X

An Improve Revocation Mechanism Using Public-Key Concept with Validation for Delay Tolerant Networks (DTN)

M.Tech.Scholar Ritika Ujjainiya
Dept.of Computer Science
SAM College of Engg & Tech.
Bhopal,Madhyapradesh,India
linkinritika@yahoo.com

Asst.prof.Tanvi Khandelwal
Dept.of Computer Science
SAM College of Engg & Tech
Bhopal,Madhya Pradesh,India
Tanu.khandewal.tanu@gmail.com

Abstract **– Delay –disruption Tolerant networks are sparse wireless network which is recently being used by the existing /current network for the purpose to connect devices or the underdeveloped area of the world that works in challenging environment. Network security protocol is always required in any of the secure area, such as military. Delay-disruption Tolerant networks are sparse wireless network which is recently being used by the existing /current network for the purpose to connect devices or the underdeveloped area of the world that works in challenging environment. Network security protocol is always required in any of the secure area, such as military. In DTN there majority of time does not exist the total path from resource to target which is leads to the difficulty of how to route the packet in such environment. Routing in such network is very difficult and for that different routing protocols are developed. In this work we discuss about various routing Strategy. DTN requires mechanism to authenticate messages at each node before forwarding it in the network. So, certificate revocation lists (CRLs) being distributed in DTN network will need to be authenticated and validated for issuer certificate authority (CA) at each node. In this study we work on CRL and update public-key collision in hash table is replaced by secure hash function algorithm SH2 with proper validation by CA. and improve network packet delivery ratio, average latency and throughput. For implementation we use the one simulator**.

Keywords- **Delay tolerant networks (DTNs), Routing, Store carry and forward etc.**

I. INTRODUCTION

Due to the rigorous operation condition and the lack of continuous network connectivity, there is a large spectrum of application which prioritizes eventual message delivery over the message delay. Network serving these kind of application are generalized as Delay Tolerant Network (DTN). kavin fall, a member of intel research group introduced the Delay Tolerant network in(2002) [6] in which they provide a network architecture and an application interface to synchronize forwarding of messages within a partition based network in which topology changes continuously and provides long delays.

It is a infrastructure less wireless network. It also experiences frequent and higher duration partitions due to nodes in DTN are intermittently connected. DTN network provides no guarantee that a path from source to destination will remain same at every time instance by which we can end that two nodes will never exist in a one connected portion of the network.As compared to Traditional Internet TCP/IP protocol which is used to set up an end to end communication path between source to destination and which assumes low error rates, low propagation delays, the maximum round trip time between any node pair in the network is not excessive and Packet drop probability is small. Unfortunately, this communication standard is not suitable in challenged or opportunistic environment such as underdeveloped region, deep space and interplanetary network in which communications are area under discussion to delays and disruption, such networks

Generally familiarity from frequent conditional partition and are known as intermittently connected networks (ICNs). Popular examples of such intermittently connected networks (ICNs) scenarios are satellites, deep space probes, Mobile Wireless Sensor Networks (MWSNs) and Sensor/Actuator Networks (SANs) deployed in extreme regions[6]. Mobile Ad-Hoc Networks (MANETs) typically consisting of nodes (e.g. GPSs, PDAs, Cellular Phones, Tracking devices, Laptops, etc). Delay tolerant networking Research Group (DTNRG)[4] study the DTN connected standards. While communication in Delay Tolerant Network the Packet transmission might result in extreme delays. The node in the delay Tolerant network has the extra limitation of

restrict buffer and there is no end to end path ever available. The exceeding circumstances leads the difficulty [5] such as end to end disconnection, Long queuing message Times, High latency, small data rate and restricted resources in terms of partial memory.

Store carry and forward conception used to provides the communication among nodes in the delay tolerant network. By this, a node in the network transfer data from one node to another. By this, any node in the network wants to send data it has to accumulate and buffered the data in the form of package. After that it carry the data until it deliver to other node successfully when they are available. for the period of the communication in DTN the reliability is accomplished by using the conception of Custody transfer mechanism. In the recent years researchers have been focused on routing problem of DTN. We have tried to categorize the different routing protocol with its advantage and drawbacks.

The rest of this paper structured as follows. In section II we discussed key properties and Application of DTN. Section III includes issues and evaluation measure of DTN. Section IV describes various routing protocol strategy and also present the comparative survey of various routing protocol with its advantage and drawbacks in table form. Section V includes conclusion.

II.KEY PROPERTIES AND APPLICATIONS OF DTN KEY PROPERTIES OF DTN

Contact between two nodes in DTN is opportunistic due to end to end disconnection problem. In such scenario, data delivery only happens when two nodes are in cont Intermittent Connection DTN is sparse mobile network in which it lacks end to end connection between nodes. This is occurring due to mobility, limited resource and network partition.

1. High Latency

In Delay tolerant network scenario, two node may never meet each other for long time[6] due to which high latency is occur.

2. Low Data Rate

When two nodes may never meet each other for long time in the network, the transmission rate of data may be considerably low and largely asymmetric with long latency of data delivery.

3. Long Queuing Delay

In DTNs, the Disconnection problem is high as compared to the conventional network. The queuing delay is the time it take to drain the queue messages ahead of the tagged on. The queuing delay also depend on the data rate and the amount of competing traffic traversing network, means queuing delay may be extremely large in worst cases e.g. : minutes, hours, and days.

4. Applications

There are various real–life application area that make use of the DTN concepts where wireless nodes, mobile or stationary, are focused to undergo extreme operational condition and/or wait for extended interval of time that exceed traditional IP forwarding times before being able to forward their data to next hop. There are many real-life applications where wireless nodes, –mobile or stationary-, are forced to undergo extreme operational conditions and/or wait for extended intervals of time that exceed traditional IP forwarding times (that are usually measured in milliseconds) before being able to forward their data to next hops. Some of these applications are -

4.1 Inter-planetary Communication [5]

Interplanetary communication is the excessive cases in which DTN can be apply. The DTN application of interplanetary network beats the traditional perimeter of TCP. The enormous space separating global artificial purposes restrict the conventional method to swap data among them or with base-stations on earth. The scientist from base location on earth can manage the action of a robot working on Mars.

4.2 Wildlife Monitoring [17]

The Zebranet project has installed a global positioning system (GPS) in a zebra collar to study the habits of zebra activities, which is one of the early DTN project and was started in 2004. Collar start every few minute to record GPS location, and every 2 h open radio function, when two collars distance is in communication range they would exchange information . After a period of time, every horse collar stores the position information of other activities. Through the zebra net project zebra's mobility, migration and interspecies are going to be investigated.

4.3 Village Network

There are many countryside communication projects in inaccessible village to make available the access to Internet. Some of the project use asynchronous transmission in order to reduce the cost of communication. The purpose of Daknet project is to enable connectivity to countryside villages with limited infrastructure established in booths in order to make available basic services such as E-mail, online banking facilities. In order to provide the communication services. between village and close to town a connection enabled vehicle passes through villages are used.

4.4 Military Application

In the Military network it can accepted in very Ad Hoc manner in which it can be used by allowing the recovery of vital information in mobile combat scenario using only irregularly connected network. To provide a standard communication in military camps which is located in very rough and difficult terrestrial spot where communication not easily possible, in such scenario DTN seems much fit to send out and accept data.

4.5 Deep Space Exploration

In the next few decades, NASA and other agencies will plan a series of projects of lunar exploration, Mars exploration and others. In September, 2003, Cisco router (CL EO) was launched by satellite to monitor disaster in UK. Till to December 2008, CL EO has done a lot of routing tests in space environment including using Saratoga protocol of bundle layer instead of pervious protocol making full use of the link source to overcome serious asymmetry link conditions. The experiment shows it is feasible to use Bundle Protocol in space.

III. ISSUES AND EVALUATION MEASURES IN DTN

1.Issues in DTN-There are many issues in Delay Tolerant Network. In which many researchers has been focused and they are

3.1 Buffer Space -In DTN network suffer from long disconnection due to which node need to store the packet for long period of time. So that, they require enough buffer space to store all message that are waiting for communication opportunities. Therefore, if buffer space of node is limited, the node buffer will be overflow due to which packet will loss.

3.2Energy-The energy is an important problem in delay tolerant network that needs to be addressed. Nodes in network may have limited energy supplies due to either mobility or disconnectiviy. Routing in DTN consumes significant amount of energy by sending, receiving, storing and as well as computation process than conventional routing technique.

So that energy efficient routing protocol should be used.3.1.3 Encounter Schedule In DTN when a node send the data from source to destination, it can wait till it encounter the destination node and after that forward the packet by direct delivery to the destination. This may take long time or may not happen because DTN suffer from disconnectivity problem [6], Network node try to communicate when opportunistic contact is obtainable. The encounter schedule is very important factor in Delay Tolerant Network. Because the delivery of messages is straightly depends upon the schedule of the encounter.

3.4 Resource Allocation-Resource allocation is a major problem in DTN. As we know Delay tolerant Network work in stressful environment where there is lack of end to end connection. The main goal of DTN is to balance the maximizing message delivery and minimizing resource consumption which are clash with each other. For example when to increase the packet delivery ratio from source to destination the best way is to distribute the multiple copies of the message in the network. But it consumes more buffer space to store each data in the node.

3.5 Reliability

Reliable delivery of packet can be achieved by ensure the triumphant and steady delivery of packet by any routing protocol that have some acknowledgement. When a packet reaches to the destination, some accepted message should be sent back from destination to source.

- Finally those constituents can be tested for Integration afterward asking for Examination Case minimization algorithms.
- Comparison of the Previously Generated Test Cases and Minimized Integrated Test cases will be Performed for Detection of Fault Tolerance and hence era of Optimal Test cases.

IV.EXISTENT WORK

The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.

One basic requirement of any cryptographic hash function is that it should be computationally infeasible to find two non-identical messages which hash to the same value. MD5 fails this requirement catastrophically; such collisions can be found in seconds on an ordinary home computer.

- The security of the MD5 hash function is severely compromised.
- A collision attack exists that can find collisions within seconds on a computer with a 2.6 GHz Pentium 4 processor (complexity of 224.1).
- MD5 was demonstrated to be still quite widely used.
- The Flame malware exploited the weaknesses in MD5 to fake a Microsoft digital signature.
- MD5 processes a variable-length message into a fixed-length output of 128 bits.

1.Public-key infrastructure (PKI

PKI is an infrastructure to manage the digital certificates. PKI provides mechanisms to generate, store, distribute and revoke the digital certificates which are means to associate the public key to a specific entity signed by a CA. A certificate authority is a trusted entity in the network which is responsible for issuing certificates. There can be different levels of CAs to issue certificates to different entities. There is one root CA to issue certificates to itself and other sub-ordinate CAs who can issue certificates to other CA as or end entities

2. Hash Function and Hash Table

A hash table is a data structure used to implement an array which can store values against some keys. It uses a hash function to compute the index of array.Ideally, each key should be mapped to a unique memory location but practically it is not possible due to hash collisions. In hash collision, different keys can be location hashed to same memory location be hashed to same memory.

International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 4, July-Aug-2018, ISSN (Online): 2395-566X

V.PROPOSED WORK

1.Proposed work and Algorithm Overview-

With a specific end goal to demonstrate our best among the accessible late calculation taken blend is of late encryption strategy for information security stockpiling and further hashing capacity procedure SHA-2 is utilizing for the dynamic honesty check process.SHA-2 contains the key length of 256 piece which isn't flimsy with the animal power assault framework.

which is the key principle purpose of the hashing plan, likewise the MAC security gave if there should arise an occurrence of encryption where the most elevated number of security is being changed. Our proposed work means to give a high-security blend approach while managing the DTN security approach, as the general strategy either work with the security encryption or hashing information check system. Therefore our proposed work inferred which take a shot at both the zone as a calculation where the information hash esteem is figured at the season of actualizing encryption and information stockpiling execution into the DTN Network.

2.We are describing SHA-2 for genration of hash values

SHA-256 calculation takes after. Note the considerable increment in blending between bits of the w [16...63] words contrasted with SHA-1.

Stage1-All factors are 32-bit unsigned whole numbers and expansion is ascertained modulo 232

Stage 2- For each round, there is one round consistent k[i] and one passage in the message plan exhibit w[i], $0 \leq I \leq 63$

Stage 3- The pressure work utilizes 8 working factors, a through h.

Stage4-Big-endian tradition is utilized while communicating the constants in this pseudocode

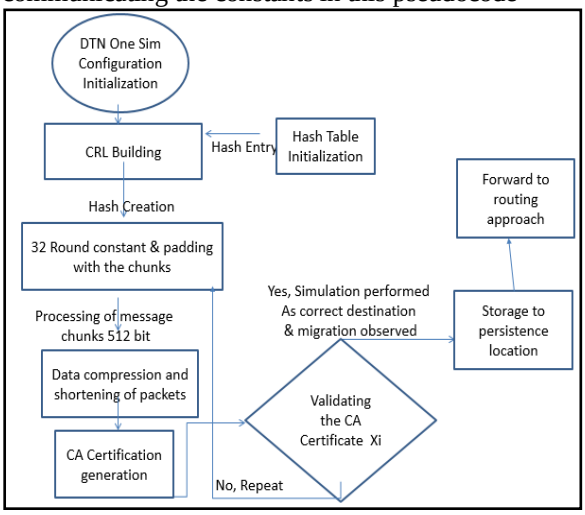

Fig.1 Flow chart of proposed Algorithm.

V.EXPERIMENTAL SETUP AND RESULT ANALYSIS

1. Simulation parameters

The simulation configuration used for the current Analysis summarized in below table.

Table1 Simulation parameter undertaken.

Parameter	Value
Duration	12h
Number Of Nodes	250
Speed Of Nodes	10-80 Km/H
Transmission Coverage	100m
Mobility Mode	Map Based Mobility
Message Size	Variable
Message Generation Interval	25-35s
Routing Protocol	Sw

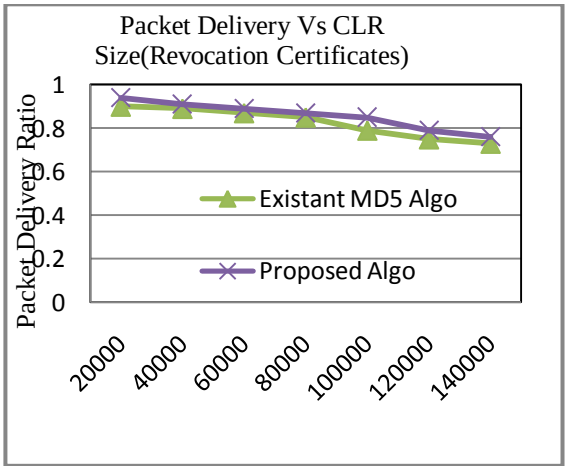

Fig.2 Packet Delivery Vs CLR Size (Revocation Certificates)

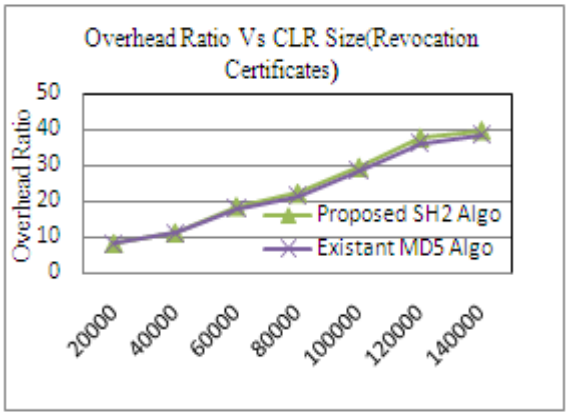

Fig.3 Overhead Ratio Vs CLR Size (Revocation Certificates)

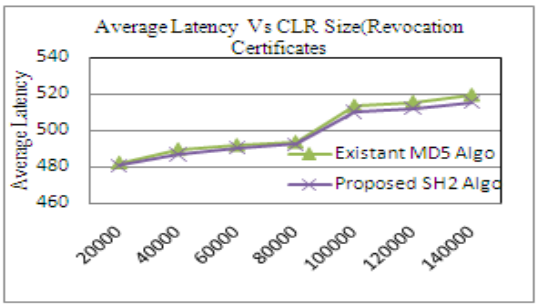

Fig.4 Average Latency Vs CLR Size (Revocation Certificates).

VI.CONCLUSION

Delay Tolerant Network is a new emerging era of intermittenly connected wireless networks. Such network operates in extreme environment where end to end communication is area under discussion to delays and disruption. It can introduce the basic idea about the origin and nature of DTN. In this paper we have focused on various routing strategy and classified the routing protocols of Delay Tolerant network into three categories: Flooding, Replication and Forwarding .Also we have presented a comparative survey of various routing protocol with their advantages and drawbacks in table. Our survey and classification facilitated us to make the following observation while designing routing protocol in DTN. Firstly, use hybrid technique and replication in order to accomplish a high delivery ratio with low utilization of resources. Secondly, routing protocol must be scalable transversely open diversity of networks in order to make available the satisfactory performance over a open diversity of Connectivity pattern. The research and development of DTN will be applied to the military war, underdeveloped region, disaster recovery, wild life tracking emergency rescue and other challenging environment.

REFERENCES

[1]. A. McMahon and S. Farell, "Distruption-Tolerant Networking," IEEE Internet Computing, vol.13, no.6, pp. 82-87, Nov.2009.Khabbaz, M.,Assi, C., & Fawaz, W. (2011).
[2]. A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," Duke university, Technically Report CS-200006,Apr. 2000.'
[3]. A. Lindgren, A. Doria, and O. Scheln. "Probabilistic Routing in Intermittently Connected Networks." LNCS, Springer, vol. 3126, pp.239-254, 2004.
[4]. Delay-Tolerant Networking Research group (DTNRG), http://www.dtnrg.org
[5]. IPN Special Interest Group (IPNSIG), http://www.ipnsig.org/
[6]. K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," in Proc. ACM SIGCOMM Conf., pp. 27-34, Aug. 2003.
[7]. Khabbaz, M., Assi, C., & Fawaz, "Distruption-Tolerant Networking: A Comprehensive Survey on Recent Development and Persisting Challenges. Communication Surveys & Tutorials", IEEE, pp(99), 1-34.
[8]. J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp:Routing for Vehicle-Based Distruption-Tolerant Networks," in Proc.IEEE INFOCOM Conf., pp.1-11, Apr. 2006.
[9]. McMahon and S. Farrell, "Delay- and Disruption-Tolerant Networking," IEEE Internet Computing, vol. 13, no.6, pp. 82-87, Nov.2009.
[10]. S. C. Lo, M. H. Chiang, J. H. Liou, and J.S. Gao, "Routing And Buffering Strategies in Delay-Tolerant Networks: Survey and Evaluation," on Proc. IEEE ICPP Workshop, Sept. 2011.
[11]. E. P. C. Jones, L. Li, And P. A. S. Ward, "Practical Routing in Delay tolerant Networks," IEEE Trans. Mobile Computing, vol. 6, no.8 pp.943-959, Aug. 2007.
[12]. R. J. D'Souza and J. Jose,"Routing Approaches in Delay Tolerant Networks: A Survey," Intl. Journal of Computer Application, vol. 1, no.17, pp. 8-14, 2010."
[13]. Z Zhang"Routing In Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant: Overviews and Challenges," in Proc. IEEE communication survey&tutorial, 1st quarter 2006.
[14]. T. Abdelkader, K.Naik, A. Nayak, N.Goel, and V. Srivastava," SGBR: A Routing Protocol for Delay Tolerant Networks Using Social Grouping,"in ieee,2012.
[15]. T. Spyropoulos, K. Psounis, and C.S. Raghav,"Single-Copy Routing in Intermittently Connected Mobile Networks,"in IEEE 2004
[16]. T. Spyroploulos, K. Psounis, and C.S. Raghavendra,"Spray and Wait:An Efficient Routing Scheme For Intermittently Connected Mobile Networks,"in Proc. ACM SIGCOMM Workshop, pp. 252-259, Aug. 2005.
[17]. The ZebraNet wildlife Tracker, http://www.princeton.edu/~mrm/zebranet.html
[18]. Shou-Chih Lo and Wei-Rong Liou,"Dynamic Quota-Based Routing in Delay-Tolerant Networks" in IEEE 2012.
[19]. S. C. Nelson, M. Bakht, and R. Kravets, "encounter- Based Routing in DTNs," in Proc. IEEE INFOCOM Conf., pp. 846-854, Apr. 2009.
[20]. E.M. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs" in Proc. ACM MobiHoc Conf., pp. 32-40 Sept. 2007.
[21]. A. Balasubramanian, B. N. Lecine, and A. Venkataramani "Replication routing in DTNs: A Resource Allocation Approach," IEEE/ACM Trans. Networking, Vol. 18, no. 2, pp. 596-609, Apr. 2010.