# An Innovative Approach For Data Transmission Based On Multiple Channels Using Distributed Time Sequence Routing Overcontent Delivery Network

**K. Rashmi Rao**
Department of Computer Science
Assistant Professor, Government First Grade College, K.R.Puram, Bangalore-36

***Abstract-*** *Internet service provider(ISP) had deployed to content delivery network(CDN) within their network infrastructure, CDN is an emerging technology with a potential application such as environment monitoring ,earthquake detection, etc., The previous work addressed the problem of overlay construction and bandwidth allocation for delivery of video channels from the entry point of the Telco-CDN to edge servers using MANETs. In this paper ,The correct relay node and sink node for data transmission is located using DTSR(Distributed Time Sequence Routing) To reduce the energy cost, nodes are active only during the data transmission and the intersection of node creates a larger merged node. Then we recognize a particular set of content delivery network applications which is to be flexible to this scalability limit, also improving the DTSR roaming with both network size and node density. The Diffie-Hellman Key Exchange is one of the more popular and interesting methods of key distribution whose sole purpose is for distributing keys, whereby it is used to exchange a single piece of information, and where the value obtained is normally used as a session key for a private-key scheme. It enables that sensor nodes can communicate each other securely. The key distribution to sensor nodes is done by means of two layer process. The paper proposes a key distribution scheme, based on intrusion detection method for using a data transmission from source to destination on the network. It is based on high level security and more energy efficient data transmission on their network.*

***Keywords:*** Transmission, Channels, Routing, Content Delivery Networks, MANET.

## I. INTRODUCTION

CDN are an emerging technology with a wide range of potential applications such as environment monitoring, earthquake detection, patient monitoring system, etc. Telecommunication networks are also being deployed for many military applications, such as target tracking, surveillance, and security management [1]. CDN typically consist of small, inexpensive, resource constrained devices that communicate among each other using a multi hop wireless network. Each node, called a telecommunication node, has one telecommunication, embedded processors, limited memory, and low-power radio, and is normally battery operated. Each telecommunication node is responsible for sensing a desired event locally and for relaying a remote event sensed by other telecommunication nodes so that the event is reported to the end user.(see fig 1.1 for CDN architecture)

The main characteristics of a CDN include

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Unattended operation
- Power consumption.

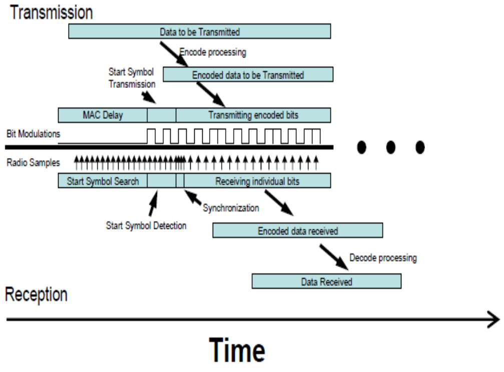

Fig 1.1Architecture Diagram for Content delivery network

The mounted upon public buses circulating within urban environments on fixed trajectory and near-periodic schedule. Namely, sinks motion is not controllable and their routes do not adapt upon specific CDN deployments. The only assumption is that telecommunications are deployed in urban areas in proximity to public transportation vehicle routes [15].

As a fair compromise between a small numbers which results in their rapid energy depletion and a large number which results in reduced data throughput. Finally, SNs are grouped in separate clusters. Raw telecommunication data are filtered within individual clusters exploiting their inherent spatial-temporal redundancy. Finally, we assume the unit disk model, which is the most common assumption in telecommunication network literature. The underlying assumption in this model is that nodes which are closer than a certain distance (transmission range R) can always communicate. However, in practice, a message sent by a node is received by the receiver with only certain probability even if the distance of the two nodes is smaller than the transmission range.

As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node’s identity; the malicious node then uses this forged identity to participate in the network routing, thus disrupting then network traffic. Those routing packets, including their original headers, are replayed without any modification. Even if this malicious node cannot directly overhear the valid node’s wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack. Since a node in a CDN usually relies solely on the packets received to know about the sender’s identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After “stealing” that valid identity, this malicious node is able to misdirect the network traffic.

For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques [1]. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could attract more than half the traffic, creating a “black hole”. This same technique can be employed to conduct another strong form of attack –[3]Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks.

The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into telecommunication networks and the hostile network condition [4]. Though mobility is introduced into telecommunication networks for efficient data collection and various applications, it greatly increases the chance of interaction between the honest nodes and the attackers. Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and an honest node with transient failure[1]. Without a proper protection, telecommunication networks with existing routing protocols can be completely overcome under certain circumstances. The emergent sensing application through Telecommunication networks saves the network from being devastated and becomes crucial to the success of the application.

## II. RELATED WORKS

Precise time synchronization is inevitable for duty-cycling and TDMA in wireless telecommunication networks. To achieve a precise synchronized clock between nodes, fast distribution of time information of a reference node to all other nodes in multi-hop without a scheduling is necessary. In this, a time synchronization algorithm, RFTS[5] (Ripple Flooding Time Synchronization), that presents the fastest distribution of time information of a reference node by using synchronized packet broadcasting instead of CSMA-CA based broadcasting.

It shows that error in any hops is not affected by a prior hop node in the evaluation, average error and distribution time of RFTS outperforms widely used FTSP[7],[2] by a factor respectively. The multi-hop routing in wireless telecommunication networks offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks and Sybil attacks.

The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing the trust-aware routing protocols do not effectively address this severe problem. To secure the Telecommunication networks against adversaries misdirecting the multi-hop routing, that has been designed and implemented TARF [5], a robust trust-aware routing framework for dynamic Telecommunication networks. Without tight time synchronization or known geographic information, this project provides trustworthy, time efficient and energy-efficient route. Most importantly, TARF [5] proves effective against those harmful attacks developed out of identity deception; the resilience of TARF [5] is verified through extensive evaluation with both implementation and empirical experiments on large-scale Telecommunication networks under various scenarios including mobile and [5] RF-shielding network conditions.

## III. PROPOSED SYSTEM

Distributed Time Sequence Routing has used to send the data efficiently and quickly on to their network[8].In this algorithm the node's direct path in the network is based on the time. DTSR protocol is to transfer the data from source to destination without any modification. Availability parameters mean connectivity and functionality in the network management layer. Connectivity is the physical connectivity of network elements. Loss is the fraction of packets lost when transmitting from sender to target during a specific time interval, expressed in percentages. The network throughput, Network delivery ratio, and availability, data loss are improved consequently, The Diffie-Hellman algorithm [18] should be used for authentication such as certificates to ensure that symmetric keys are established between nodes. The steering metrics are evaluated in dissimilar literatures to indicate the significance and measuring purpose of frequent routing protocols. In absolute surveys all along with the classification of these metrics by means of their meticulous classifications are discuss in detail.

The module is developed for the wireless network requirements, wireless equipment's, Transmitter and receiver between one to another node to calculate the distance. Wireless telecommunication transmission ranges cover all nodes. Telecommunication networks most often have a much more complicated topology than the simple examples and not all telecommunication nodes can communicate with each other directly. Thus, multi-hop synchronization is required, which adds an additional layer of complexity. Clearly, it could be avoided by using an overlay network which provides virtual, single-hop communication from every telecommunication node to a single master node. DTSR is a reactive time synchronized protocol, which can be used to obtain times of event detections at multiple observers in the local time of the sink nodes. Provides a more detailed description of the protocol later when formally analyze the time synchronization errors it introduces.

The steps involved in the key structure is given below, (ref fig 3.1)

**Step 1**
The network has multiple client and server
**Step 2**
If
Client node wish to send the data then it check the neighbor node

If it is free means then transfer the data in that server.
Else
It doesn't send the data and again check for the free neighboring node.
**Step 3**
The server nodes will response to all the client nodes.
**Step 4**
If DDoS attack occurs in the server node means then the server will response only to the particular client in the network.
**Step 5**
Using this response the client access the another server in the network.

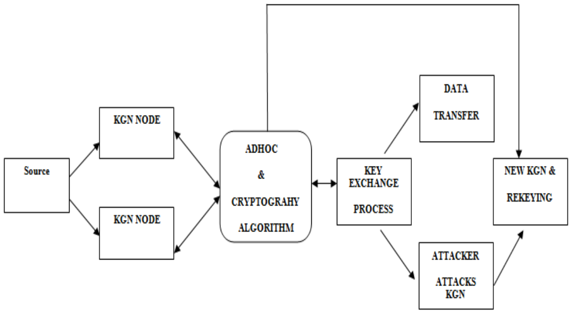

Fig 3.1 Architecture for key structure.

## IV. EVALUATION

Extensive simulations are conducted to evaluate the performance of the proposed solutions in this paper.
The following 3 metrics are used in our comparisons:

### A. Throughput ratio

In computer networks, throughput is the amount of packet that a network can transfer it in a given time period.
Throughput: rate (bits/time unit) at which bits transferred between sender/receiver.

$$\text{Throughput ratio} \leq \frac{RWIN}{RTT}$$

Where RWIN is the TCP receive window and RTT is the round-trip time for the path.

### B. Packet loss ratio

Packet loss occurs when one or more packets of data travelling across a network fail to reach their destination. Packet loss is typically caused by network congestion.

Packet loss is measured as a percentage lost with respect to packets sent.
To calculate the packet loss,

$$\lambda P_{blk}$$

If to calculate the average rate of admitted packet then do

$$\lambda(1 - P_{blk})$$

Knowing the P(n) probabilities you can calculate $P_{blk}$as

$$P[x(t) = k] = (1 - \rho)\rho k$$

## C. Delay ratio

The delay is the time a packet waits in a queue until it can be forwarded, So end to end delay (t):

Nodal delay

$$d_{nodal}=d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

$d_{proc}$ = Processing delay (typically a few microseconds or less)

$d_{queue}$ = Queuing delay (depends on congestion)

$d_{trans}$= Transmission delay (significant for low speed links)

$d_{prop}$= Propagation delay (a few microseconds to hundreds of microseconds)

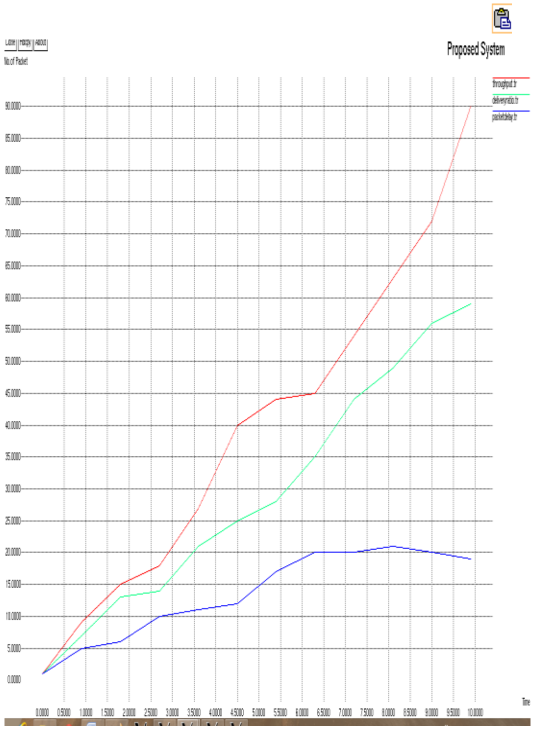

Fig 4.1 Performance of the proposed system

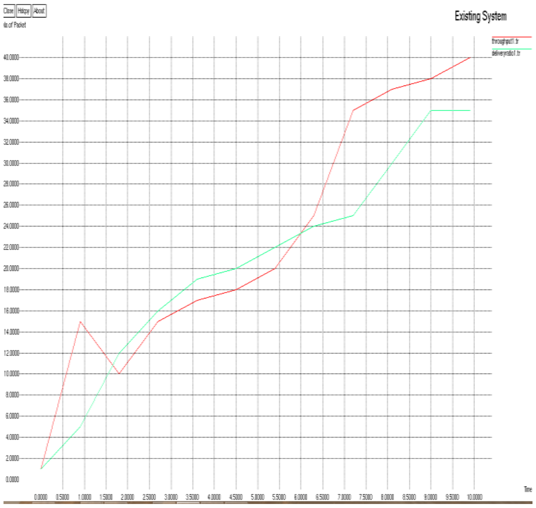

Fig 4.2 Performance of existing system

The table for evaluating the performance ratio is given (in table 4.1)

The joint optimization reveals that the ratio of delivered channels are efficient by using the heuristics algorithm but their bandwidth consumption is not minimized as expected but by using the DTSR and Deffie-Hellman key exchange the system is secured and the bandwidth consumption is minimized as expected which it results in good performance of the system.

Table 4.1 Performance ratio

| **Algorithm** | **Throughput ratio** | **Delay ratio** | **Packet loss ratio** |
|---|---|---|---|
| **Joint optimization** | 90.5% | 70.78% | 84.3% |
| **DTSR** | 96.2% | 96.5% | 95.2% |

## V. CONCLUSION

The information based metric, entropy, is applied for final filtering of suspicious flow. Trust value for a client is assigned by the server based on the access pattern of the client, and updated every time when the client contacts the server. Diffie-Hellman Key swap is one of the most well-liked and interesting method of key sharing.

It is a public-key cryptographic system whose sole reason is for distributing keys, whereby it is used to swap over a single piece of information, and anywhere the value obtained is in general used as a sitting key for a private-key system. It enables that adhoc nodes can converse each other securely. As a future work, the proposed system is planned to implement in the real time video streaming systems.

## REFERENCES

[1] Joint optimization for the delivery of multiple video channel in Telco CDNs by Fen Zhou,Jiayi Liu,GwendalSimon and RoaofBoutaba in IEEE 2015

[2] Time synchronization in wireless sensor networks by Srikandan Kumar 212CS2108 NIT, Rourkela in 2014

[3] Lightweight Sybil attack detection in MANETs by Sohailabbas,MadjidMerabti,David Llewellyn-Jones and KashifKifayat in IEEE Systems journal,vol-7,No.2 2013

[4] Detecting the Sybil attack in mobile adhoc networks by Chris piro,Clay Shields and Brian Neil Levine in NSF grants CN0133055, CNS-0834618,and CNS-0087639 2013

[5] Identifying trusted routing path in WSNs through TARF by S.Anitha,A.Nithya and A.Vijay in ICCTET 2013

[6] Optimization of Content Caching in Content-Centric Network. Tuan-MinhPham,Michel Minoux ,Serge Fdida, MarcinPilarski in 2013

[7] Model-Checking the flooding time synchronization protocol by A.I.Mclnnes in Control and automation 2009

[8] Distributing Content Simplifies ISP Traffic Engineering.BhigyanSharmay,ArunVenkataraman, Ramesh K Sitaramany in IEEE WIRELESS MAGAZINE ,2007 The Economic Impact of Telco CDNs and their Alliance on the CDN Market Hyojung Lee, Dongmyung Lee, and Yunog Yi IN KCA 2013

[9] Pushing CDN-ISP Collaboration to the Limit. Benjamin Frank, Ingmar Po,Georgios,Smaragdak,AnjaFeldma, BruceJannis Rake,Steve Uhlig,Rick Weber In ACMsigcomm computer communication review, 2013

[10] Video Delivery over Heterogeneous Cellular Networks - Optimizing Cost and Performance KonstantinosPoularakis, George Iosifidis, AntoniosArgyriou, and LeandrosTassiulasIn swisscom and Akami enter into a strategic partnership,March 2013

[11] Joint Optimization of System Lifetime and Network Performance for Real-Time Wireless Sensor Networks Lei Rao 1, 2, Xue Liu 2, Jian-Jia Chen 3, Wenyu Liu Huazhong University of Science and Technology, Wuhan in FQRNT grant 2010-nc-131844

[12] “Tree-based Group Key Agreement” Yongdae Kim, Adrian Perrig, and Gene Tsudik,2011

[13] “Securing Body Sensor Networks: Sensor Association and Key Management” SyeLoongKeoh, Emil Lupu and Morris Sloman 2010

[14] “Reliable Network Connections” Victor C.Zandy and Barton P. Miller,2010

[15] Jointly optimizing data acquistion and delivery in traffic monitoring VANETs”

[16] “Anonymity and Security in Delay Tolerant Networks” Aniket Kate, Greg Zaverucha, and UrsHengartner, 2008

[17] “Security Issues in the Diffie-Hellman Key Agreement Protocol” Jean-Fran¸cois Raymond and Anton Stiglic,2008

[18] “Weaknesses in two group Diffie-Hellman key exchange protocols” Qiang Tang, Liqun Chen, 2006

[19] “Wireless Sensor Network Security: A Survey” John Paul Walters, Zhengqiang Liang 2006

[20] “Key agreement in peer-to-peer wireless networks” Mario ˇCagalj, SrdjanCapkun and Jean-Pierre Hubaux.