

# Design and Analysis of Hybrid Software Defined Network System for Stability Enhancement

J. Jeyarani<sup>1</sup>, R. Deepalakshmi<sup>2\*</sup>, R. Vanitha<sup>3</sup>, M. Shivashankari<sup>4</sup>, S. Shanthi<sup>5</sup>

<sup>1,2,3,4,5</sup>Department of ECE, CARE College of Engineering, Tiruchirappalli, Tamilnadu, India

\*Corresponding Author: [rdeepalakshmi@care.ac.in](mailto:rdeepalakshmi@care.ac.in), Mob: 8344898019

Received: 20/May/2022, Accepted: 15/Jun/2022, Published: 30/Jun/2022

**Abstract**— Software-defined networks (SDNs) facilitate more efficient routing when traffic flows using centralized network view. On the other hand, traditional distributed routing still has the advantage of better scalability, robustness, and swift reaction to events such as failure. Therefore significant potential benefits to adopt a hybrid operation where both distributed and centralized routing mechanisms co-exist. This hybrid operation however imposes a new challenge to network stability since a poor and inconsistent design can lead to repeated route switching when the two control mechanisms take turns to adjust the routes. In this paper, we discuss the ways of solving the stability problem. To develop the stable networking environment three tier routing architecture is proposed. The router stability is enhanced and speed of data transfer is high in this proposed system. The router will analyze the network traffic that occurs during the data transfer and redirect to the other router. The algorithms used in this proposed systems are Support vector machine algorithm and Multilayer perception algorithm. The stability of a hybrid-software defined network involves the consistency between the centralized routing performed by the centralized controller and the distributed routing performed by the individual local routers. If these two control units are not consistent with each other, the routing decision may be overturned repeatedly as they take turns to modify the routes.

**Keywords**— ANN, Software-defined networks (SDNs), Support vector machine algorithm, Multilayer perception algorithm, Bandwidth enhancement

## I. INTRODUCTION

A network is any collection of independent computers that communicate with one another over a shared network medium. A computer network is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives. When networks at multiple locations are connected using services available from phone companies, people can send e-mail, share links to the global Internet, or conduct video conferences in real time with other remote users. When a network becomes open sourced it can be managed properly with online collaboration software. As companies rely on applications like electronic mail and database management for core business operations, computer networking becomes increasingly more important.

Network can be divided in to two main categories:

- Peer-to-peer.
- Server – based.

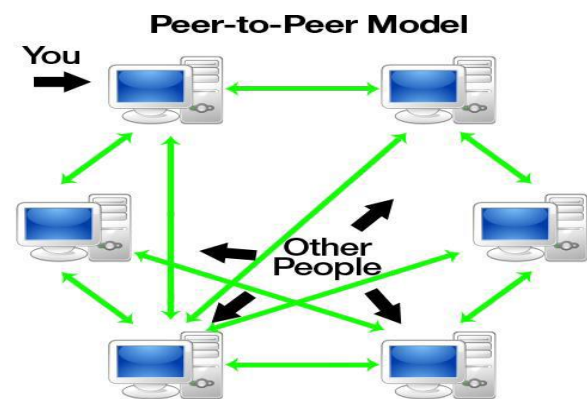


Fig.1 Peer to Peer Model

In peer-to-peer networking as in Fig.1, there are no dedicated servers or hierarchy among the computers. All of the computers are equal and therefore known as peers. Normally each computer serves as Client/Server and there is no one assigned to be an administrator responsible for the entire network. Peer-to-peer networks are good choices for needs of small organizations where the users are allocated in the same general area, security is not an issue and the organization and the network will have limited growth within the foreseeable future. The term Client/server refers to the concept of sharing the work involved in processing data between the client computer and the most powerful server computer.

## II. LITERATURE REVIEW

Broad casting is an effective mechanism for route discovery, but the routing overhead associated with the broadcasting can be large, especially in high dynamic networks. The protocol analytically and experimentally, and showed that the rebroadcast is very costly and consumes too much network resource. Optimizing the broadcasting in route discovery is an effective solution to improve the routing performance. Network density is high or the traffic load is heavy, the improvement of the gossip-based approach is limited, proposed a probabilistic broadcasting scheme based on coverage area and neighbor confirmation. Coverage area to set the rebroadcast probability, and uses the neighbor confirmation to guarantee reach ability. Scalable Broadcast Algorithm (SBA) is rebroadcast of a packet according to the fact whether this rebroadcast would reach additional nodes. Dynamic Probabilistic Route Discovery (DPR) is based on Neighbor coverage and each node determines the forwarding probability according to the number of its neighbors and the set of neighbors which are covered by the previous broadcast [1]. A dynamic probabilistic broadcasting approach with coverage area and neighbor confirmation, the coverage area concept to adjust the rebroadcast probability of a node. One of the earliest broadcast mechanisms is flooding, where every node in the network retransmits a message to its neighbors upon receiving it for the first time. Although flooding is extremely simple and easy to implement, it can be very costly and can lead to serious problem, named as broadcast storm problem, which is characterized by redundant packet retransmissions, network bandwidth contention and collision. Neighbor knowledge scheme maintains neighbor node information to decide whether it or the neighboring nodes have to rebroadcast or not. To use neighbor knowledge method, each node has to explicitly exchange neighborhood information among mobile hosts using periodic Hello packets. Four different gossip versions are presented for ad hoc routing (GOSSIP1 (p, k), GOSSIP2 (p1, k, p2, n), GOSSIP3 (p $\psi$ k $\psi$ m) is just like GOSSIP1 (p $\psi$ k), GOSSIP4 (p $\psi$ k $\psi$ k') is just like GOSSIP1 (p $\psi$ k)). In general, Neighbor knowledge methods perform better than Area based methods, while Area based methods perform better than Probability based methods. An important problem is how to minimize the number of rebroadcast packets while good retransmission latency and packets reachability are maintained. Even though the large number of rebroadcasts guarantees high reachability, it causes high network bandwidth wastage and so many packets collisions [2]. Routing overhead associated with the dissemination of routing control packets such as RREQ packets can be quite huge, especially when the network density is high and the network topology frequently changes. Issue of reducing the routing overhead associated with the route discovery and maintenance processes in on-demand routing protocols has attracted increasing attention. Location Aided Routing (LAR) algorithm as an approach to mitigate the route discovery overhead by utilizing location aided information for mobile nodes,

location information can be obtained using the global positioning system (GPS) receivers. The localization of prior routing histories to localize the RREQ flood to a limited region of the network, Routing On-demand Acyclic Multi-path (ROAM) protocol mitigates the number of retransmissions of RREQ floods by using directed acyclic sub-graphs based upon the distance between the source and destination nodes. The construction and maintenance of virtual backbone that guarantees total coverage of the entire network is either based on Connected Dominating Set (CDS) or Cluster based algorithms. A predefined probability value to decide whether or not to forward an RREQ packet. Some optimizations such as two-threshold scheme (i.e. use higher probability value for nodes with fewer neighbors) are introduced to prevent broadcast packets from quickly dying out and/or prevent nodes from transmitting excessive packets. A dynamic probabilistic route discovery using AODV as the base routing protocol, which traditionally uses the blind flooding. In order to reduce the routing overhead without degrading the network throughput, especially in dense networks, the forwarding probability of nodes located in sparse areas is set high while it is set low at nodes located in dense areas [3]. Gossiping to ad hoc unicast routing, it's usage of gossiping is very different from the work, try to ensure that messages are eventually delivered, even if there is no connected path between the source and the destination at any given point in time. Exists a path using communication links at some point in time, messages can be delivered through a random pair-wise exchanges among mobile hosts. Using gossiping mechanism to improve multicast reliability in ad hoc networks, they do not use gossiping to reduce the number of messages sent. Flooding is a basic element in many of the ad hoc routing protocols, as mentioned and comparing gossiping to flooding. Protocol is simple and easy to incorporate into existing routing protocols, by adding gossiping to AODV, significant performance improvements in all the performance metrics, even in networks as small as all nodes [4]. Single Administrative Domain (SAD) involved operations refer to operations where all involved parties belong to the same regime or share a common, predefined point of trust. Multiple Administrative Domains (MAD) involved operations represent operations involving ad hoc partners, that have had no prior contact and belong to different organizational/security domains. Key management operations should finish in a timely manner despite a varying number of nodes and node densities, fraction of the available bandwidth occupied by network management traffic should be kept as low as possible. Any increase in management traffic reduces available bandwidth for payload data accordingly. Wired network solution is a public key infrastructure (PKI) where a centralized certificate authority (CA) issues certificates binding the public keys to specific users/nodes. Self-Healing Session Key Distribution (S-HEAL) is a symmetric group key-distribution scheme with revocation, designed for networks with unreliable links. Logical Key Hierarchy (LKH) Group keys can be updated brute force; a group manager distributes the new group key, encrypted with a separate

(individual) key for each node. Probabilistic Key Pre-distribution (PRE) assumes WSN nodes outfitted with a preinstalled key ring, that is, a set of keys drawn randomly from a large pool of keys. When bootstrapping the network, the nodes broadcast the identifiers of the keys in their key ring. Classify key-management schemes for MANETS (mobile ad hoc networks) as either contributory or distributive. Distributive schemes based on symmetric techniques are either intended for traditional MANETs or for wireless sensor networks (WSNs). Observation is that none of the proposed key-management schemes for MANETs are truly effective for all MANET scenarios [5]. Ad-Hoc network security schemes which utilized certificates that rely on hierarchical trust model, do not explicitly address the issue of certificate revocation, Other proposals such as make the assumption that periodic access to on-line CAs is available; therefore CRLs can be obtained from the CAs. In Buchegger and Le Boudec proposed the CONFIDANT protocol that is aimed at detecting and isolating misbehaving nodes, methodology for actually computing the trust level or rating of the nodes within a MANET. A number of reputation systems have been published in research literature, systems can be divided into two main types: centralized and distributed reputation systems. Centralized reputation systems require central authorities for collecting the rating of participants and derive reputation scores. Centralized reputation systems are not suitable for MANETs since MANETs do not have centralized entities. The majority of proposed decentralized reputation systems are transactional based; that is, they require inputs, such as size of upload or down files, quality, price and upload/ download experiences relating to interactions of providers of services and users of the services. Our scheme stipulates that before entering a network, the MANET nodes must have a valid certificate from a recognized CA, as well as the public keys of the CAs which issued certificates for potential network peers. This paper Presented a decentralized certificate revocation scheme which utilizes certificates that are based on the hierarchical trust model and Delegates all key management tasks except the issuing of certificates—to the nodes in a MANET and it does not require any access to on-line certificate authorities (CAs) and Certificate revocation scheme is based on weighted accusations; whereby a quantitative value is assigned to an accusation to determine its weight [6].

### III. EXISTING SYSTEM

Single tire architecture is been implemented for data transfer using the network topology. The consistency and throughput of the data in the network is quite low. Greedy Kernel Algorithm is implemented in the existing system. Software-defined networks (SDNs) facilitate more efficient routing of traffic flows using centralized network view. On the other hand, traditional distributed routing still enjoys the advantage of better scalability, robustness, and swift reaction to events such as failure. There are therefore significant potential benefits to adopt a hybrid operation where both distributed and centralized routing mechanisms

co-exist. The key management problem is an active research area in wireless sensor networks. Proposed a probabilistic key pre distribution scheme to bootstrap the initial trust between the sensor nodes. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key.

#### Disadvantages

- Low speed in data transfer
- Throughput is minimum
- Computation time is high
- Security thread is high
- Data is no security
- Attacker is very easily
- ABE Algorithms is encryption file is very poor

### IV. PROPOSED SYSTEM

In the proposed system the three tire routing architecture is implemented for the stable node transformation. The router will analyze the network traffic that occurs during the data transfer and redirect to the other router. The algorithms used in this proposed systems are Support vector machine algorithm and Multilayer perception algorithm. The stability of a hybrid-software defined network involves the consistency between the centralized routing performed by the centralized controller and the distributed routing performed by the individual local routers. If these two control units are not consistent with each other, the routing decision may be overturned repeatedly as they take turns to modify the routes. Before proceeding to the dual control consistency, we should specify the underlying assumption about the behavior of local routers to ensure the stability of the distributed routing.

#### Advantages

- High speed in data transfer
- Throughput is maximum
- Computation time is very low
- No Security thread issues

#### 4.1 SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

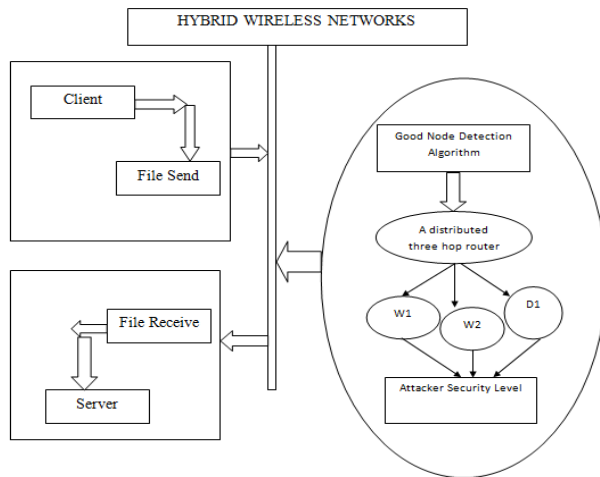


Fig 4.1.1 System Architecture

#### 4.2 MODULES

- Source node
- Destination node
- Routing Stability
- Hybrid Three tier security
- Router Information
- Load on throughput

##### Source node

A client is an application or system that accesses a server on computer system, known as a server, by way of a network. The Client machine is always used for sending data/file request to the server machine. Client-server computing or networking is a distributed application architecture that no of node partition tasks or workloads between service providers (servers)-500MB. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await incoming requests.

##### Destination node

A server is any combination of software designed to provide services to clients. When used alone, the term typically refers to a computer which may be running a server operating system, but is commonly used to refer to any software or dedicated hardware capable of providing services to the requesting client.

##### Routing Stability

Software-defined networks (SDNs) facilitate more efficient routing of traffic flows using centralized network view. On the other hand, traditional distributed routing still enjoys the advantage of better scalability, robustness, and swift reaction to events such as failure. Stability for hybrid SDNs and then establish a per-priority stabilizing framework to obtain stable routing patterns.

##### Hybrid Three tier security

The hybrid three-tier security scheme provides better

network resilience against mobile sink replication attack compared to the ANN approach. This scheme delivers the same security performance as the ANN when the network is under a stationary access node replication attack. In both schemes, for any sensor node  $u$  that needs to authenticate and establish a pair wise key with a stationary access node  $A$ , the two nodes must share at least a common ANN. To perform a stationary access node replication attack on a network, the adversary needs to compromise at least a single ANN from the static pool.

##### Router Information

In the network be given a routing table and a link table. Analyze the security performance of the proposed scheme against a routing stability replication attack. Routing Energy level & Stability level increase the report.

##### Load on throughput

Investigate the effect of traffic load on throughput for our proposed ANN the traffic is also generated based on variable-bit-rate applications such as file transfers over Transmission Control Protocol (TCP). The average packet size is 1,000 bytes, and source-destination pairs are chosen randomly with uniform probabilities.

#### 4.3 SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, Sub-assemblies, assemblies' and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test type addresses a specific testing requirement.

##### TESTING STEPS

- Unit Testing
- Integration Testing
- Functional testing
- System testing
- White Box testing
- Black Box testing
- Output Testing

##### Unit Testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

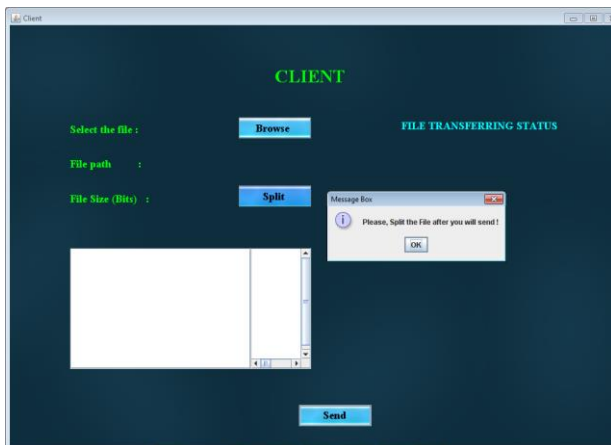


Fig.4.4.1 Transmission of file

### Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfactory, as shown by successful unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

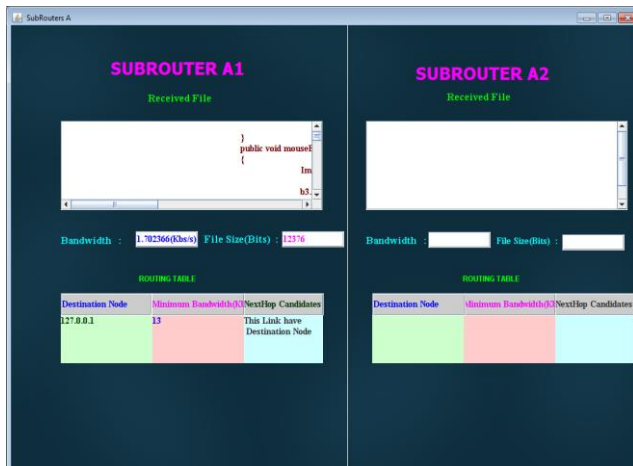


Fig.4.4.2 File transmitted in the Sub routers

### V. CONCLUSION

We defined stability for hybrid SDNs and then established a peer-priority stabilizing framework to obtain stable routing patterns. For each priority class, we discussed global optimization, greedy, and local search approaches to reach hybrid SDN stability. We designed and implemented a system on a centralized controller which utilizes kernels to stabilize the Software defined Network. This hybrid operation however imposes a new challenge to network stability since a poor and inconsistent design can lead to repeated route switching when the two control mechanisms take turns to adjust the routes the stability problem. The proposed local search provides the best

tradeoff among cost performance, computational complexity, and route disturbance compared to the existing systems.

### VI. FUTURE ENHANCEMENT

As the future research work, we proposed to design a Multitier architecture system which will transfer the secured data. Delay will be reduced during the phase of n-architecture decision. It could be more efficient to improve n-architecture performance in Multitier architecture.

### REFERENCES

- [1] Mohammad Al-Fares, Sivasankar Radhakrishnan, Barath Raghavan, Nelson Huang, Amin Vahdat, "Hedera: Dynamic Flow Scheduling for Data Center Networks", Proc. USENIX NSDI, pp. 89–92, 2016.
- [2] V. Mann, A. Vishnoi, K. Kannan, and S. Kalyanaraman, "Seamless VM mobility across data centers through software defined networking", Proc. IEEE/IFIP NOMS, pp. 88–96, Apr. 2017.
- [3] A. Iyer, P. Kumar, and V. Mann, "Data center multicast using software defined networking", Proc. IEEE COMSNETS, pp. 1–8, Jan. 2018.
- [4] C.Y. Hong et al., "Achieving High Utilization with Software-Driven WAN", ACM SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, pp. 15–26, 2018.
- [5] S. Jain, A.M. Hegland, E. Winjum, "Experience with a globally-deployed software defined WAN", ACM SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, pp. 3–14, 2018.
- [6] C. J. S. Decusatis, A. Carranza, and C. M. Decusatis, "Communication within clouds: Open standards and proprietary protocols for data center networking", IEEE Commun. Mag., vol. 50, no. 9, pp. 26–33, Sep. 2018.
- [7] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: Dynamic flow scheduling for data center networks," in Proc. USENIX NSDI, pp. 89–92, 2010.
- [8] V. Mann, A. Vishnoi, K. Kannan, and S. Kalyanaraman, "CrossRoads: Seamless VM mobility across data centers through software defined networking," in Proc. IEEE/IFIP NOMS, pp. 88–96, Apr. 2012.
- [9] A. Iyer, P. Kumar, and V. Mann, "Avalanche: Data center multicast using software defined networking," in Proc. IEEE COMSNETS, pp. 1–8, Jan. 2014.
- [10] C.-Y. Hong et al., "Achieving high utilization with software-driven WAN," ACM SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, pp. 15–26, 2013.
- [11] S. Jain et al., "B4: Experience with a globally-deployed software defined WAN," ACM SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, pp. 3–14, 2013.
- [12] C. J. S. Decusatis, A. Carranza, and C. M. DeCusatis, "Communication within clouds: Open standards and proprietary protocols for data center networking," IEEE Commun. Mag., vol. 50, no. 9, pp. 26–33, Sep. 2012.
- [13] M.F. Bari et al., "Data center network virtualization: A survey," IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 909–928, 2nd Quart., 2013.
- [14] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey," IEEE Commun. Mag., vol. 51, no. 11, pp. 24–31, Nov. 2013.
- [15] D. Kreutz, F. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.
- [16] M. Yu, J. Rexford, M. J. Freedman, and J. Wang, "Scalable flow-based networking with DIFANE," ACM SIGCOMM Comput. Commun. Rev., vol. 40, no. 4, pp. 351–362, Oct. 2010.

- [17] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, "DevoFlow: Scaling flow management for high-performance networks," *Comput. Commun. Rev.*, vol. 41, no. 4, pp. 254–265, Aug. 2011.
- [18] S. Sezer et al., "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013.

#### AUTHORS PROFILE

*Dr.J.Jeyarani* pursued Bachelor of Engineering Bharathidasan University Trichy in 1999, Master of Engineering in Anna University Chennai in year 2007 and Ph.D. in National Institute of Technology Trichy in 2019 and currently working as Associate Professor in Department of Electronics and Communication Engineering in CARE College of Engineering, Trichy, Tamilnadu since 2019. She is a member of IEEE since 2021, a life member of the IETE, BES since 2009. She has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. Her main research work focuses on Optical Communication, Free Space Optics and Antennas. She has 20 years of teaching experience and 5 years of Research Experience.

