Semiconductor Optoelectronics
ISSN: 1001-5868

CLOUD BACKED OPTIMAL GATEWAY DETECTION TECHNIQUE IN AN INTEGRATED INTERNET – MANET

Atma Prakash Singh
Ph.D. Research Scholar, Maharishi University of Information Technology Lucknow

Dr. Santosh Kumar
Professor, Maharishi University of Information Technology Lucknow

Abstract : A common trend is that the quality of service starts to deteriorate when the certain gateway is connected with large of number of mobile devices. Thus we are proposing that the threshold number of mobile devices up to which certain gateway works well within the expectations could be found and such number could be called as capacity for that gateway. After that in the optimal gateway discovery protocol, before connecting any node to the gateway its capacity should be checked for the optimal results. Decentralized, self-organized networks, such as dedicated cellular operators and dedicated vehicle networks, might benefit from trust-based systems to safeguard against insider assaults.. Encryption and access control in A/V can be used to protect against external threats. Prevention-focused systems such as cryptographic safeguards are often ineffective against malicious insiders. Trust, as defined under the Trust Management Framework, is the degree to which an observer trusts an organization to act in an ethical manner. Instead, innovation-based methods such as trust management predict the behaviour of internal nodes in real time.

Key Words : Cloud computing , MANET, NFV.

1. Introduction : Ad hoc networks have been developed over the years and are used in both military and civilian environments. The evolution of ad hoc networks will affect people's ways of life in the future. As an example of how MANET can be used to improve people's daily commutes, think about how people's perceptions of road conditions have changed. Meanwhile, innovations such as network function virtualization are causing fundamental change in the way networks are designed and managed. The ad hoc network service and architecture have been improved, accelerating the development of ad hoc network applications. One day, all digital software will have dedicated networking capabilities. It is common for people to use services without giving much thought to the networks and/or technologies that make this possible. Dr. Mark Weiser, an early advocate of pervasive computing, claimed that the "peaceful technological age, when technology recedes into the background of human life," [3] has arrived. In order to provide the best possible service, the provider must ensure that their customers do not know how their data is being sent or stored. The day will come when IT help

will be as common as cable or telephone. There is no shortage of supply, it's always there so no one notices it doesn't exist.To achieve this ambitious goal, security in computer networks should be prioritized as a research field. A variety of security issues affect the architecture of each layer in each type of network, from wired and centralized to decentralized, mobile, and self-organizing wireless networks. As our modern and interconnected society increasingly relies on the Internet, security has become an increasingly important issue since its rapid ascent in the 1990s. Many cryptographic research efforts have been made to find solutions to these security problems, and the resulting techniques are often referred to as prevention-based mechanisms or hard protection systems. Attackers will always find a way to circumvent security measures, no matter how well designed they are. If hackers can bypass the network's first defences, these measures will be ineffective. As a result, soft protection technologies (detection-based technologies) are created to further improve network security. Over the past few years, trust-based systems have received considerable attention as a potentially profitable innovation-based strategy for network security. Here are four important advantages of trust-based systems.

2.Cloud Computing and NFV in MANET:

Cloud computing's flexibility and adaptability mean that even the tiniest businesses may eventually make use of the same resources that were formerly reserved for the larger ones. Because of this, using computers is both straightforward and energy-efficient [4]. Because of its adaptability to satisfy the fluctuating needs of the market, cloud computing is increasingly being seen as a public utility.

The word "cloud" must be defined before any discussion of "cloud computing" can begin. Using "an infrastructure that contains both computer hardware and the operating systems and applications that operate on that hardware," [5] is how the term "cloud computing" is defined. Without the hardware and software that powers the data centre, the cloud would be useless. Customers may be required to pay a fee if the data centre’s owner decides to restrict access to certain apps. The cloud computing community has settled on three common service categories [6]. "Software as a service," or SaaS, refers to a model in which software is hosted remotely and made available to users through the internet. One such service is Dropbox [7], which allows users to store and share files on the cloud. Customers may choose from a number of storage packages that range in price. As a version control service, GitHub is available [8]. Businesses of various sizes, not to mention independent programmers and open-source communities, purchase project management services from the software industry. Cloud-based application creation, deployment, and management are made possible to some part by "platform as a service" (PaaS). A good example is Google's App Engine [9], which offers a server platform for customers to host Java, Python, or PHP programs. Customers that use Infrastructure as a Service have access to every utility. Accessing cloud services does not restrict the operating system a user may be using. Windows Azure [10] provides this kind of service and is capable of running a wide variety of operating systems to meet the needs of its users. All of these different categories of cloud services depend significantly on virtualization. The networking sector will undergo significant changes as a result of NFV. Because it gives telecommunications firms, who play a crucial role in the network service business, the

flexibility to meet the evolving demands of their clientele. There is also the flexibility for NFV-based network services to suit the needs of the future.

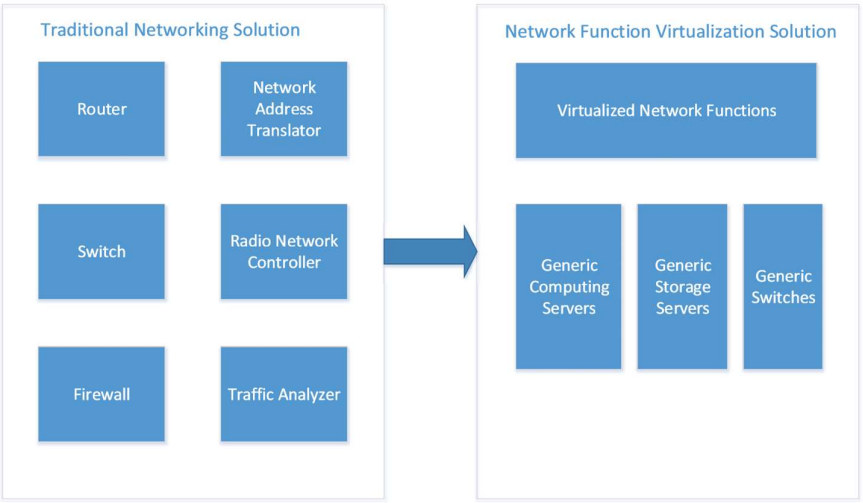

Figure 1: The transition from traditional networking hardware to NFV reduces costs [1]. NFV allows for fine-grained customisation and software-like flexibility in the delivery of network services. By increasing the scalability of network services, Network Function Virtualization (NFV) paves the way for the implementation of new business models.

By using a network hypervisor [11] similar to a virtual machine's hypervisor, NFV moves the core network functions formerly incorporated into network devices to the higher-level software. By virtualizing networks, we may be able to get a fresh perspective on these systems. In other words, it "digitizes" the real-world asset [12]. With abstraction, slicing, isolating, and sharing, even the most fundamental of physical networks may be virtualized. The NFV design may be seen in Fig. 1. Commercial value is brought to the customer through the network service. This component includes all the functionality required and meets all the requirements. Network services need NFV management and orchestration in order to create and convert to lower layer VNFs. Virtualized network functions (VNFs) include firewalls and routing protocols. Each VNF's deployment and management is handled by a VNF life-cycle manager. The VNF life-cycle management allocates resources to each VNF during deployment. Aside from that, the VNF life-cycle management monitors

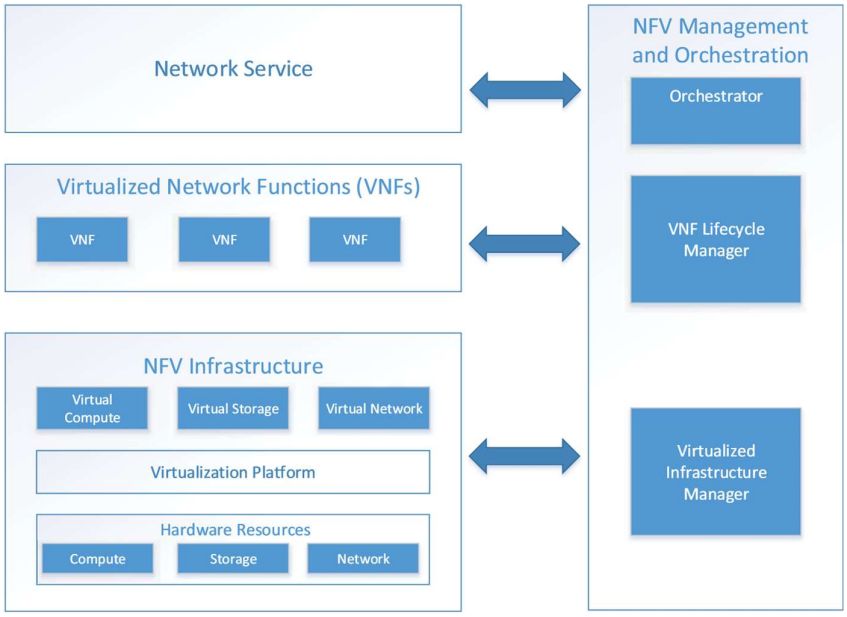

Figure 2.: Organizational Network Function Virtualization Architecture [2].

In general, VNFs. Corrective actions and VNF scalability adjustments may be implemented through the VNF life-cycle management. NFV management and orchestration rely on the VNF life-cycle manager to carry out business logic. Provisioning of additional virtual resources including computation, storage, and network is made possible thanks to the NFV infrastructure module's backing of VNFs. An essential part of the NFV architecture, the virtualization platform abstracts away the need for physical resources. The term "hypervisor" is occasionally used to describe this level. OpenStack [6], VMware vCenter [7], and Amazon Web Services [8] are all parts of this framework. The virtualized infrastructure manager is a piece of software responsible for overseeing the NFV infrastructure.

3.Result and Conclusion: Create a MANET using the proactive demand affirmation routing protocol, and then use GloMoSim to facilitate peer-to-peer communication within the ad-hoc network. Before choosing an intergateway connection, the gateway is examined without the use of a central administration. Send the client (the vehicle node) to the gateway first, and if you receive an acknowledgement and can locate it nearby, you can send the vehicle node a request to get data and receive an acknowledgement that is tied to a routing table or register. Request messages CV REQ GW are broadcast to all gateways within the client mobile's or client vehicle's (CV) hearing range. When a request is made, the gateway closest to the client responds and chooses to act as the internet portal up until it becomes overloaded, at which point it sends the requesting client an acknowledgement message (GW ACK). The closest gateway is chosen as the optimal gateway to service the client vehicle after it is overloaded. Then CV sends a message with the request for data CV REQ DATA through the chosen gateway. The ACK DATA message is sent by the cloud to inform the requesting CV whether the requested data is available or not. When the client vehicle is prepared to accept data and receives acknowledgement, it sends the message CV RDY DATA to the cloud.Following that, Table

driven (Proactive) Routing protocols—On demand (Reactive) Routing protocols—list out destinations routing by regularly dispersing routing tables demand by flooding Apply all of these techniques to the MANET network and measure the following parameters using the calculations.

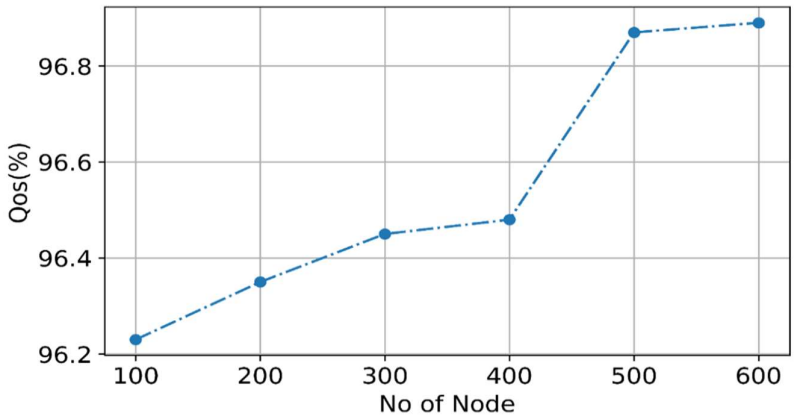

Figure 3. -#QoS qos=(PacketShaper/10)*100Quality of service vs no of node

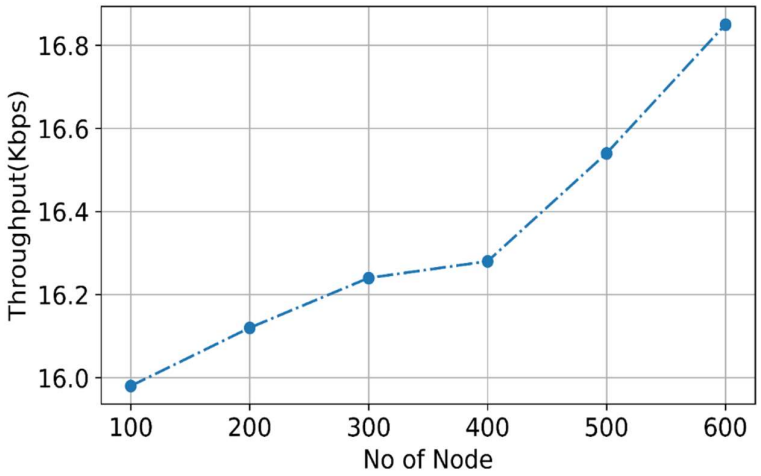

Figure 4. network end to end delay vs no of nodedely=Length of packets

Following that, Table driven (Proactive) Routing protocols—On demand (Reactive) Routing protocols—list out destinations routing by regularly dispersing routing tables demand by flooding Apply all of these techniques to the MANET network and measure the following parameters using the calculations.

4.References:

[1] "Network functions virtualisaztion (NFV); NFV security; problem statement." website: http://www.etsi.org.

[2] "Network functions virtualisaztion (NFV): Architectural framework." website: http://www.etsi.org.

[3] M. Weiser, "The computer for the 21st century," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 3, pp. 3–11, July 1999.

[4] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[5] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," *IETF RFC 3626*, Oct. 2003.

[6] T. Clausen, C. Dearlove, and P. Jacquet, "The optimized link state routing protocol version 2," *IETF draft-ietf-manet-olsrv2-13*, Oct. 2011.

[7] "Qualnet simulator." website: http://www.scalable-networks.com/content/.

[8] D. Heckerman, "A tutorial on learning with bayesian networks," *Microsoft Research Report MSR-TR-95-06*, 1995.

[9] M. Momani, S. Challa, and R. Alhmouz, "BNWSN: Bayesian network trust model for wireless sensor networks," in *Proc. MIC CCA'08*, (Amman), Aug. 2008.

[10] C. T. Nguyen, O. Camp, and S. Loiseau, "A Bayesian network based trust model for improving collaboration in mobile ad hoc networks," in *Proc. IEEE Research, Innovation and Vision for the Future*, (Hanoi, Vietnam), Mar. 2007.

[11] Y. Wang and J. Vassileva, "Bayesian network trust model in peer-to-peer networks," in *Proc. AAMAS'03*, (Melbourne, Australia), Jul. 2003.

[12] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, 1988.

[13] G. Shafer and J. Pearl, *Readings in Uncertain Reasoning*. Morgan Kaufmann, 1990.

[14] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proc. ACM AAMAS'02*, (Bologna, Italy), Jul. 2002.

[15] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using DempsterShafer theory," in *Proc. IEEE Instrumentation and Measurement Technology Conf.*, (Alaska, USA), May 2002.

[16] J. Y. Halpern, *Reasoning about Uncertainty*. The MIT Press, 2003.

[17] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Proc. IEEE MilCom'09*, (Boston, MA, USA), Oct. 2009.

[18] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile Ad Hoc Networking: The Cutting Edge Directions, 2nd Edition*. Wiley-IEEE Press, 2013.

[19] J. Loo, J. Lloret, and J. H. Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends*. CRC Press, 2011.

[20] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for ipv4," *IETF RFC 4728*, Feb. 2007.

[21] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," *IETF RFC 3561*, Jul. 2003.

[22] T. Clausen, C. Dearlove, and J. Dean, "Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)," *IETF RFC 6130*, Apr. 2011.

[23] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR protocol," in *Proc. 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2003)*, (Mahdia, Tunisia), Jun. 2003.

[24] T. Clausen and U. Herberg, "Vulnerability analysis of the optimized link state routing protocol version 2 (OLSRv2)," in *Proc. IEEE WCNIS'10*, (Beijing, China), Feb. 2010.

[25] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Comm. Mag.*, vol. 40, no. 10, pp. 70–75, 2002.

[26] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: distributed key management for security," in *Proc. 2nd OLSR Workshop*, (Domaine de Voluceau, France), Dec. 2005.

[27] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, "Data communication in MANET," *Ad Hoc Netw.*, vol. 44, pp. 90–103, July 2016.

[28] J. M. III, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. KTH, 2000.

[29] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, pp. 50–58, Apr. 2010.