ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Secured & Clustered Fail-over Routing in Tethernet

Garima Bhalla, Mahesh Singh

M.Tech Student, Dept. of CSE., Advanced Institute of Technology and Management (MDU), Palwal, India

Asst. Professor, Dept. of CSE., Advanced Institute of Technology and Management (MDU), Palwal, India

ABSTRACT: Wi-Fi tethering (i.e., sharing the Internet connection of a mobile phone via its Wi-Fi interface) is a useful functionality and is widely supported on commercial Smartphone's. Yet existing Wi-Fi tethering schemes consume excessive power: they keep the Wi-Fi interface in a high power state regardless if there is ongoing traffic or not. In this paper we propose System to improve the Fail over cluster routing with security in Wi-Fi tethering. Based on measurements in typical applications, we identify many opportunities that a tethering phone could carry over the transmission even one or more nodes go off/shutdown in tether-net. We design a secured failover protocol/approach to coordinate the nodes and schedule the perfect data transmission of the tethering phone with its clients without requiring tight time synchronization using Route Discovery Protocol and Crank Bank enabling Fail over Routing with Secured Transmission. Furthermore, we develop a two-stage, secured and fail over adaptation algorithm to automatically adapt the failover of node to ongoing traffic patterns of various applications, ensuring the 100% data transmission on time to the clients with security. However, system does not require any changes to the 802.11 protocol and is incrementally deployable through software updates. We have implemented System on commercial Smartphone's. Experimental results show that, while retaining comparable user experiences, our implementation can allow the Wi-Fi interface to sleep for up to 88% of the total time in several different applications, and reduce the failover transmission by 99.99% under the restricted programmability of current Wi-Fi hardware.

KEYWORDS: Tether-net, Clustering, Failover, Security, RDP, 802.11, Crank Bank.

I. INTRODUCTION

Wi-Fi tethering, also known as a "mobile hotspot", means sharing the Internet connection (e.g., a 3G/4G connection) of an Internet-capable mobile phone with other devices over Wi-Fi. As shown in Figure 1, a Wi-Fi tethering mobile phone acts as a mobile Wi-Fi tethering software access point). Other devices can connect to the mobile through their Wi-Fi interfaces. The mobile Wi-Fi tethering with t routes the data packets between its 3G/4G interface and its Wi-Fi interface. Consequently, all the devices connected to the mobile Wi-Fi tethering are able to access the Internet.

Figure 1: Wi-Fi tethering.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Wi-Fi tethering is highly desired. For example, even before the Android platform provided built-in support on Wi-Fi tethering, there were already some third-party Wi-Fi tethering tools on Android Market. Two of them, called "Barnacle Wi-Fi Tether" and "Wireless Tether for Root Users", are very popular, each with more than one million installs. There are two main reasons why Wi-Fi tethering is desirable. First, cellular data networks provide ubiquitous Internet access but the coverage of Wi-Fi networks is spotty. Second, it is common for people to own multiple mobile devices but likely they do not have a dedicated cellular data plan for every device. Hence, it is desirable to share a data plan among multiple devices, e.g., sharing the 3G/4G connection of an iPhone with a Wi-Fi only iPad.

In response to this common user desire, Wi-Fi tethering is now widely sup-ported, as a built-in feature on most smart phone platforms, including iPhones (iOS 4.3+), Android phones (Android 2.2+) and Windows phones (Windows Phone 7.5).However, existing Wi-Fi tethering schemes significantly increase the power consumption of Smartphone's. When op-rating in the secured mode, the Wi-Fi interface of Smartphone is always put in the high end data transmission and denial state even when there is no data traffic going on. These in-creases the power consumption by one order of magnitude and reduces the battery life from days to hours to ensure the 100% secured data transmission between two nodes or clients. Clustered Failover is a procedure by which a system automatically transfer control to a duplicate system when it detects a fault or failure and to ensure the transmission is between the trusted clients it ensure the security standards for rest and fully fledged successful transmission. It is a backup operational mode in which the function of a system component example server, network, database, and processor are summed by a secondary system component, when primarily components become unavailable through failure. It is used to make system more faults tolerant. It can be applied to any aspect of a system within a PC, within a network, to any network component or system of component such as connection path, storage device etc. In this work I have created secured clustered failover routing that works when a master node about to fail while transmitting packets to a slave node due to low energy or faults then it transfers its control to the other node and request that node to transfer the remaining packets to the slave node on its behalf. Hence by this we can assure the data transmission with security. In this proposed work, the transmitting node will send frame sets to the other node after it has stopped due to power loss or any fault. The other node will only send the remaining file to the receiving node. Hence it prevents the stoppage of transmission occurring due to less power which is caused because of the continuous active involvement of the node in the network formed by tethering.

II. RELATED WORK

Route Discovery with Role Protocol the double-role device is with lower performance. Thus, we propose a crank-back routing to resolve the double-role node on a route. The crank-back routing employs the route discovery with role protocol RDRP as shown in Fig. 2. In the routing table, every device will be associated with a role parameter. For the backbone route, each device is with a specific role. When the on-demand route is established, the route reply packet is sent from the destination and the bridge that receives the route reply packet will compare its role with the role recorded in the route reply packet for this device.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

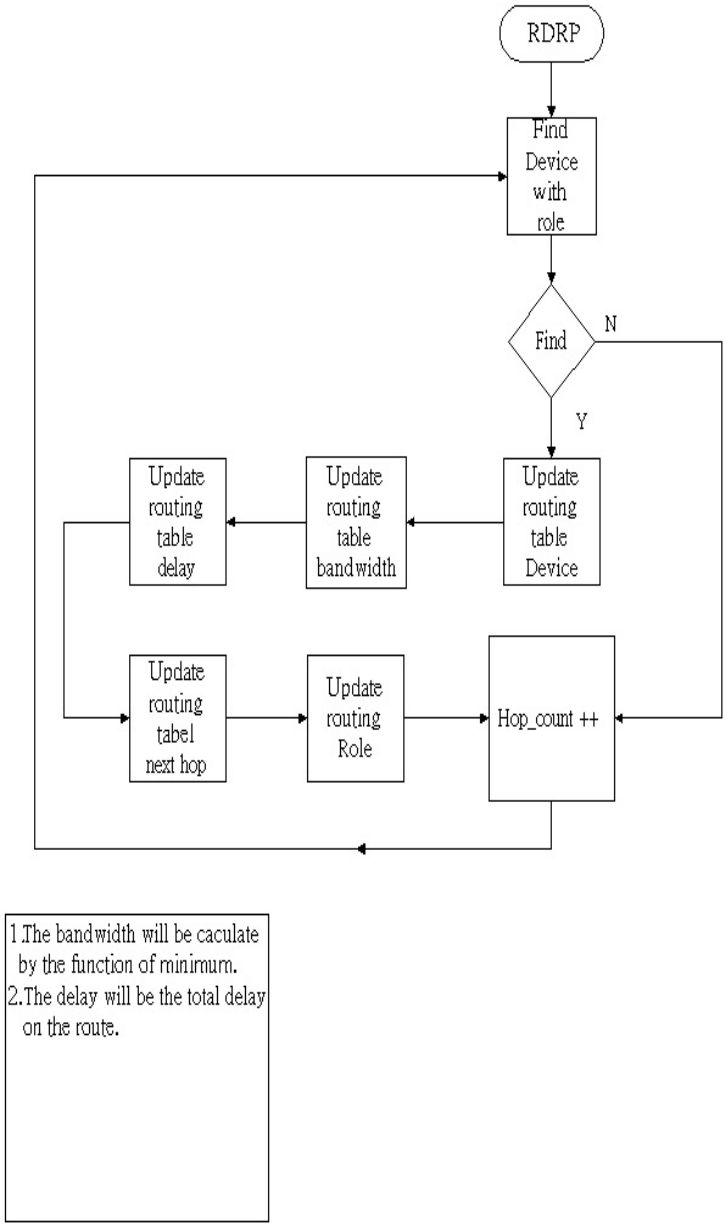

Fig 2: Route Discovery with Role Protocol

If the role for the device on the route is the number 0, it knows that it is a master. However, if the role number is 1, it means that the device is a slave on the route. When a device is associated with two roles (both the master and the slave), it is a double-role device. When the new bridge knows that it is not a master, it will cancel the crank-back procedure and tell the device that initiates the crank-back routing to find another route. If the procedure falls into a loop, the new crank-back route can't be established. Then, a time limit is set to resolve the infinite loop issue. If the time limit expires, the new route is not established. Then, the original route that is with a slave or double-role devices is still used for data transmission.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. PROPOSED WORK

To evaluate the performance of the proposed secured clustered fail over routing, we develop a simulation model and conduct simulation study with desired results.

Model Proposed

The following notations are used in this study.

D_i : end-to-end delay for secured route

B_i : the route of bits per second through

t_s : the length of a time slot (i.e., 0.625)

t_g : guard time for a bridge switching among ethernet

N_i^n : the number of nodes on route

N_i^b : the number of bridges on route

L : is the length of the packet size (2745bits)

e_m : the number of masters on the endpoints of

We can calculate the end-to-end delay and the bandwidth by using Eq. (2) and Eq. (3).

$$D_i = \begin{cases} 2t_s\left(N_i^n - 1\right) + N_i^b\left(t_g + t_p\right), & for \quad 1 - slot \\ 4t_s\left(N_i^n - 1\right) + N_i^b\left(t_g + t_p\right), & for \quad 3 - slots \\ 6t_s\left(N_i^n - 1\right) + N_i^b\left(t_g + t_p\right), & for \quad 5 - slots \end{cases} \tag{2}$$

$$B_i = \begin{cases} \dfrac{L}{2t_s\left(N_i^n - 1\right) + N_i^b\left(t_g + t_p\right)}, & for \quad 1 - slot \\ \dfrac{3L}{4t_s\left(N_i^n - 1\right) + N_i^b\left(t_g + t_p\right)} & for \quad 3 - slots \\ \dfrac{5L}{6t_s\left(N_i^n - 1\right) + N_i^b\left(t_g + t_p\right)} & for \quad 5 - slots \end{cases} \tag{3}$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

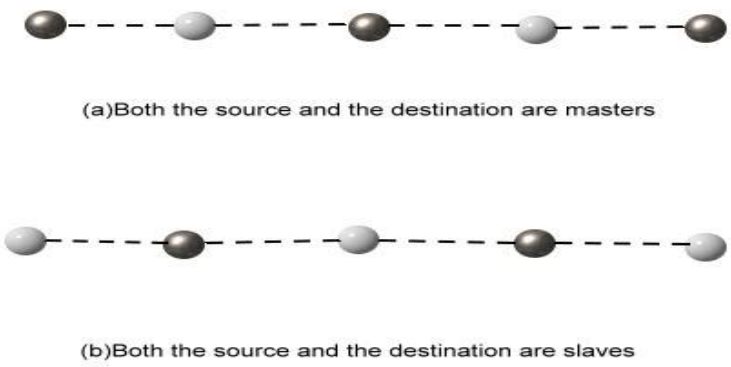

Figure 3: The number of nodes along the route is odd

We make the following assumptions for this simulation study. (i) We assume that the number of nodes on the route is odd in order to simplify the study. In other words, the source and the destination devices are either two masters or two slaves as shown in Figure 3 (a) and Figure 3 (b), respectively. And the number of nodes on the route that we would like to evaluate is from 5 to 39. Thus, the value of in our study is either 0 or 2, and we can figure out the number of bridges on according to Eq. (4).

$$N_i^b = \frac{1}{2}\left(N_i^n - 3 + e_m\right) \qquad (4)$$

For example, the route shown in Figure 3.5.1-(a) has two slave bridges to connect three Tether-net. We can substitute by 5 and by 2 into Eq. (4) to calculate the value of to be 2 (bridges). The other assumptions are as follows.

1. There is no error occurring during data transmission and, thus, the retransmission is not required.
2. The guard time is considered as the worst case, i.e., two time slots ($t_g = 2t_s$).
3. We assume that the scheduling is perfect. In other words, when a bridge switches from a Tether-net to the other Tether-net, it requires only two time slots (guard time) to adjust its radio frequency to a new frequency according to the new hopping sequence. And the master polls the bridge immediately for data transmission.
4. The traffic on R_i is unidirectional.
5. The number of intersections on a route is proportional to the length of the route. Though the above assumptions much simplify the study, it does not lose the generality and fairness and can provide us with a quick evaluation of the performance of Tether-net routes thus ensuring the 100% data transmission on Tether-net.

IV. PROPOSED SECURITY ALGORITHM

1. **Key Generation (by Master)**
   i. The signer randomly selects two large primes p1 & p2 such that
   n = p1 * p2

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

p = 2n + 1 & p is prime

ii. Then signer generates his private keys x, r & public keys as

y = gx mod p &

h = gr mod p, where g is a large prime selected by signer randomly.

iii. Then he sends public keys set (p , g , y , h , n) to the requester for blinding.

2. **Sightless (by Node):** Suppose a requester want to obtain a signature on message m. Then

i. He generates private keys a, b & w randomly & computes

U1 = H (h ga yb mod p, m) mod n, where H is a cryptographic hash function

U2 = U1 + b mod n

K = gw mod p

3. **Signing (by Master):** After receiving u2 from requester, the signer computes Z = (r + u2 x) mod n & sends z to requester.

i. After receiving z, the requester computes

Z' = Z + a + w mod m

ii. Then he sends (Z' , u, k) as the blind signature on message m, to the receiver.

4. **Verification (by receiver):** The signer's authenticity can be verified by checking the following equation

H(gz' (y)-u1 k-1 mod p, m)mod n = U1 mod n

V. RESULTS

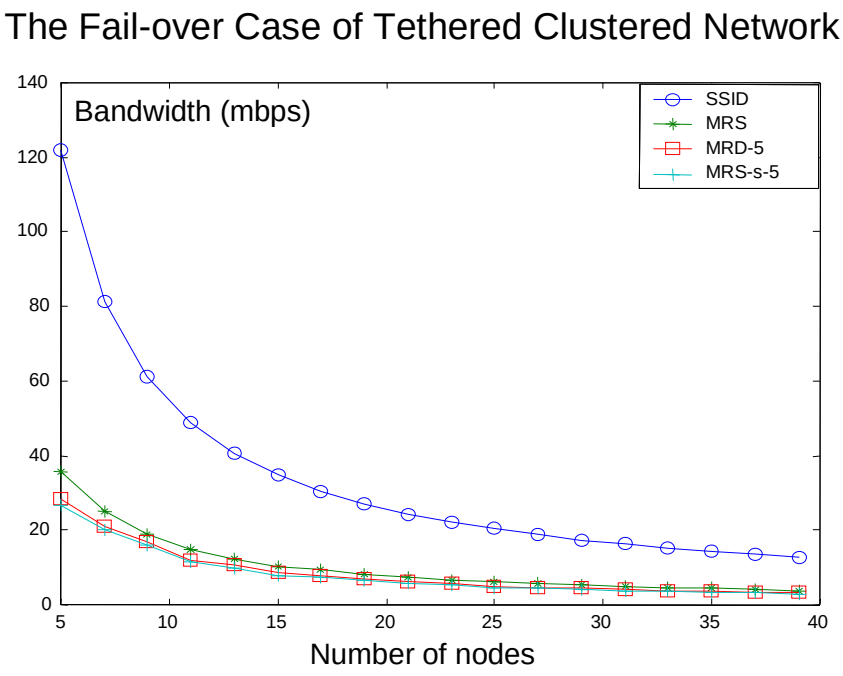

Fig 4: Secured Fail over Cluster comparison.

In scheme there is only one tethered network. Tethering is done and all the mobile devices are connected with each other via Wi-Fi hot spot. All the devices which are connected via hotspot must possess same SSID and different MAC. The whole process is done at background not at the foreground so that it may be incorporated with security. In this

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

whole process, we are having a mobile phone which is acting as a server and computer as clients using sockets for fetching the data. It sends the request to the server for sending that file but if the power back up of the server is not good or insufficient then the client's request is broadcasted to the other nodes/server who all are present in that tethered network. Now the node that is having sufficient power back up will act as a master and send the file to the client over a cluster over secure channel. Whereas in MRS (Master Relay Services) the non-secured and clustered exists and MRD (Master Relay Domain) is a cluster which is damaged due to collision or node failures. Consequently, the entire transmission terminated and MRS resumes the transmission again to from the network from beginning.

VI. CONCLUSION

Tethernet is a network that allows sharing of internet connection of phones with other devices such as laptops. Failover is a procedure by which a system automatically transfers control to a duplicate system when it detects a fault or failure over the network. Wi-Fi has better performance in terms of energy as compared to Bluetooth but also has disadvantage that it increases the power consumption as in this mode Wi-Fi interface is always put in in high power state reducing the battery life of the phones. The secured failover routing prevents the stoppage of transmission if the transmitting node about to fail. It will pass its control to another node and allow it to transmit instead of it. The on-demand routing provides the suitable route to transmit. When one node stops while transmitting, it will send the frame sets to the other node and ask it to send the remaining frame sets within secured environment

ACKNOWLEDGMENT

I sincerely thank my guide, Mr. Mahesh Singh, for his constant support during my work. I would also like to thank my fellow classmates for fruitful discussions and valuable suggestions.

REFERENCES

[1] Ashish Sharma, Vishnu Navda, Ramachandran Ramjee, Venkata N. Padmanabhan and Elizabeth M. Belding, Cool-Tether: Energy Efficient On-the-fly Wi-Fi Hot-spots using Mobile Phones in Proceeding CONEXT'09, Proceeding of the 5th International Conference on Emerging Networking Experiments and Technologies 2012.
[2] Pering, T. Agarwal, Y. Gupta, and Want, CoolSpots: Reducing the Power Consumption of Wireless Mobile Devices with Multiple Radio Interfaces, In MobiSys, June 2009.
[3] Jelena Mi˘sic´, Vojislav B. Mi˘sic´, "Bridges of Tethering County: Topologies, Scheduling, and Performance," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 21, NO. 2, FEBRUARY 2006.
[4] Hao Han, Yunxin Liu, Guobin Shen, Yongguang Zhang and Qun Li, DozyAP: Power-Efficient Wi-Fi Tethering. Networking, IEEE/ACM Transaction, Vol 22, issue: 5, 2013.
[5] Kyoung-Hak Jung, Yuepeng Qi, Chansu Yu and Young-Joo Suh, Energy Efficient Wi-Fi Tethering on a Smartphone, INFOCOM, 2014 Proceedings IEEE, 2014.
[6] L.M. Freeny, "Energy efficient communication in ad hoc networks" Mobile Ad Hoc Networking, Wiley-IEEE press, pp. 301-328.2004.
[7] P.K.Sahoo, J.P.Shehu and K.Y.Hsieh, "Power control based topology construction for the distributed wireless sensor networks", Science Direct, Computer Communications, vol. 30, pp. 2774-2785, June 2007.

BIOGRAPHY

Garima Bhalla is an M.Tech student in the CSE Department, Advanced Institute of Technology and Management (MDU), Palwal, India. She received Bachelors of Technology (B.Tech, CSE) degree in 2012 from Les Filles MVN (MDU), Palwal, India. Her research interests are Computer Networks (wireless Networks), Algorithms, Mobile development etc.

.