RESEARCH ARTICLE OPEN ACCESS

Securing The Channels Between Core Nodes In Y-Comm Framework

Hossam Adel Abdel Fattah, Dr. Ahmed Abdel Hafez, Prof. Abdel Hamid A. Gaffar

Communication Dept. Arab Academy for Science and technology, Cairo, Egypt
Communication Dept. Military Technical College Cairo, Egypt
Communication Dept. Arab Academy for Science and technology, Cairo, Egypt

Abstract
Future Generation Networks are the Networks that had the ability to work with all the available Wireless Technologies and in the same time support the best Qos and experience for the end user. The openness of the future Networks Architecture (Heterogeneous Networks) will have new security threats that need to be addressed due to the network architecture change. In this paper, these security threats in the AKA protocol will be addressed for the Y-comm framework. Moreover, the problem of having insecure channels between Core Nodes that leads to a lot of security threats will be investigated. Finally, a new proposal by including Authentication and Encryption module in the main protocol will be presented. This module was simulated using CASPER and successfully Verified using formal methods of FDR

Keywords— heterogeneous networks; Y-Comm framework; security; Future Networks;

I. INTRODUCTION

The wireless technologies are rapidly evolving from 2G and 3G to LTE(Long Term Evolution) and WIMAX. all of these upgrades are concentrated in terms of bandwidth and QoS . These systems are running in different Domains which means that they are running with different management systems like (MME, MSC, and SGSN). So the Evolved Packet Core (EPC) [1] was made with the idea of flat architecture [2] and upgrading the PS Domain without changing the CS domain. It can be considered as migration steps towards one management system in future Networks. the Future Networks should select the best type of Access from available wireless technologies (2G, 3G, LTE, WIMAX). the network should determine the best QoS and Trusted systems to pick from these supported technologies. Also these technologies could be supported from any operator, so the operators must cooperate with each other to model the Open Architecture future networks.

Open Architecture networks will have new threats rather than the old threats modeled for the old Network. This is a result from the fact that the network will be no longer closed by operators but it will be accessible to other Networks and intruders. Security threats for open network architecture (heterogeneous networks) should be checked.

The new architecture for heterogeneous networks that put into consideration the security, handover and QoS are:

1. the Mobile Ethernet as described in [5], [6].
2. Ambient Networks Explained in [9].
3. IEEE 802.21 [7], [8]
4. the Y-Comm framework [4].

Y-Comm supports full integration and introduces a well-structured communication framework [4]. The AKA protocol was used with Y-Comm Framework to model the openness of the Network. Security threats was checked using simulation Casper language[15,16] and verified using FDR (Failures Divergence Refinement) [11] . analysis made to the results of Casper/FDR to solve the threats found[3].

In This paper, the insecure communication between Core Nodes leads to multiple attacks and threats. The threats should be solved after securing the channels between the core nodes.

Section I is the introduction which will discuss the background and paper Structure. Section II discuss different architecture that can support open networks structure. the investigation was made with comparing the integration of Qos ,Security , Mobility for different systems . Introduction for Y-Comm Framework and it's Architecture. Section III describe security threats on Y-Comm framework and how to overcome this threats. Section IV is the verification for the proposed solution using Casper/FDR. Section V is the Conclusion.

II. PREVIOUS WORK

Mobile networks are evolving to meet users expectations with the Best Qos. Networks with Different Technologies should be allowed to

cooperate with each other to ensure the best Qos for the user in that sense. cooperation between network technologies can be made if the network architecture is open. Open architecture needed to accept all types of wireless technologies and from different operators to guarantee the best Qos for user. This networks should not scarify Security or Mobility Management. The Open Networks Architecture (Heterogeneous networks) are the idea for using the network resources whatever the type of technologies. the possible communication architectures for heterogeneous networks are the Mobile Ethernet [5] [6], Ambient Networks [9], IEEE 802.21 [7] [8] and the Y-Comm framework [4]. As mentioned on [4] the Y-Comm Framework is one of the solutions that integrate the Qos along with Security and Mobility. Y-Comm deals with the Qos and Security as they are related to each other .
the network structure of the Y-comm is described as shown on the below figure (1) [4], [14], [13]

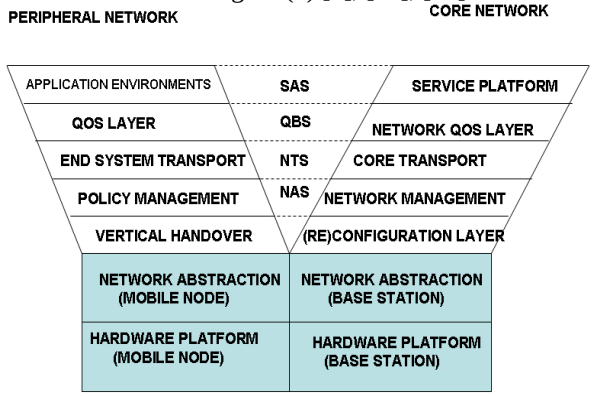


Fig. 1 Y-Comm Framework

There are 2 networks as shown above
- The Peripheral Network: deals with operations on the mobile terminal.
- The Core Network : deals with functions in the core network to support different peripheral networks.

These Networks are brought together to represent a future telecommunication environment. Which supports heterogeneous devices, disparate networking technologies, network operators and service providers. The Peripheral and the Core Networks share the Hardware Platform and the Network abstraction layer. Both Networks diverge in terms of functionality, but the corresponding layers interact to provide support for heterogeneous environments.

A. The Peripheral Network

The Peripheral Framework is concerned with activities on mobile nodes and in the wireless networks to which they are connected. The peripheral framework has seven layers:

1. *The Hardware Platform Layer (HPL):* It is used to classify all relevant wireless technologies. Hence different wireless technologies which are characterized by the electromagnetic spectrum, MAC and modulation techniques make up this layer.
2. *The Network Abstraction Layer (NAL):* It provides a common interface to manage and control different wireless technologies. The first two layers for both frameworks are similar in functionality. In the Peripheral Framework, they run on the mobile terminal to support the various wireless network technologies. while in the Core Framework these two layers are used to control the functions of base stations of different networks.
3. *The Vertical Handover Layer (VHL):* This layer executes vertical handover. Therefore, this layer acquires the resources for handover, initial handover signaling, context transfer and packet reception after vertical handover.
4. *The Policy Management Layer (PML):* The PML decides whether, when and why handover should occur. This is done by looking at various parameters related to handover. such as signal strength and using policy rules to decide both the time and place for doing the handover.
5. *The End Transport Layer(ETL):* It allows the mobile node to make end-to-end connections across the core network. This layer provides the functionalities of the Network and Transport layers of the TCP/IP module.
6. *The QoS Layer (QL*): In the Peripheral Framework, it supports two mechanisms for Handling QoS. The first is defined as Downward QoS. The application specifies its required quality-of-service to the system and the system attempts to maintain this QoS over varying network channels. The other definition is Upward QoS, where the application itself tries to adapt to the changing QoS. This layer also monitors the QoS used by the wireless network as a whole to ensure stable operation.
7. *The Applications Environments Layer (AEL):* It specifies a set of objects, functions and routines to build applications which make use of the framework.

B. The Core Network

This framework deals with functions in the core network. The first two layers of the Core Frameworks are shared with the Peripheral framework. The remainders layers are:

1. *The Reconfiguration Layer (REL):* It is responsible for managing key infrastructure such as routers, switches, and other mobile network

infrastructure using programmable Networking techniques.

2. *The Network Management Layer (NML):* The NML is a management plane that is used to control networking operations in the core. This layer divides the core into a number of networks which are managed into an integrated fashion. It also gathers Information on peripheral networks such that it can inform the policy management layer on mobile nodes about wireless networks at their various locations.
3. *The Core Transport System (CTS*): It is concerned with moving data through the core network.
4. *The Network QoS Layer (NQL*): It is concerned with QoS issues within the core network especially the interface between the core network and the peripheral networks.
5. *The Service Platform Layer (SPL*): This layer allows services to be installed on various networks at the same time.

As shown in Fig 1, Y-Comm deploys a multi-layer security module which must be applied to both the Peripheral and Core Framework simultaneously to provide total security. The security layers must work together across both frameworks
in order to be fully integrated with the new architecture. The
security module comprises four layers:

1. *Service And Application Security (SAS):* authenticates the user to use the mobile terminal.
2. *QoS Based Security:* looks at QoS issues, e.g., Service Level of Agreements (SLA), network overloading and Denial of Service Attacks (DoS) in both the core and peripheral networks.
3. *Network Transport Security (NTS*): sets a secure session between the mobile terminal and the end server.
4. *Network Architecture Security (NAS):* it defines the security issues and threats resulting from moving to a particular network type.

The architecture proposed in [12] for the Y-comm shown below in Fig. 2.

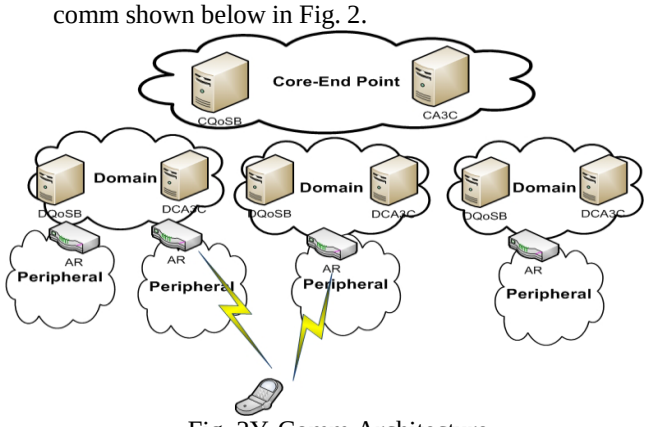


Fig. 2Y-Comm Architecture

The top level is the Core End-Point (CEP) which acts as a gateway to the Internet and is responsible for managing multiple, mid-level domains. Each domain is technology-specific and is controlled by a single operator.

- *Core A3C (CA3C):* The top level A3C server resides in the Core End-Point and is Responsible for service level management with security info. It holds the subscribed services along with the associated QoS and networks or the Operators, the user can access with the corresponding QoS.
- *Core QoS Broker (CQoSB):* managing inter-CEPs functions as Well as negotiating QoS parameters with other CQoSBs in the case of cross Core End-Points connection. The CQoSB initially extracts users' Level of Agreement from the CA3C.
- *Domain A3C (DA3C):* The DA3C is responsible for handling users' service Requirements initially. it extracts users' profile information from the CA3C and uses this information for authorizing the users' requests to access services.
- *Domain QoS Broker (DQoSB):* gets user's profile information from the CQoSB and manages the resources of the attached peripheral networks with respect to the user preferences and network availability. it also makes a per-flow admission control decision. In order to support handover.
- *Access Router (AR*): This is the link between the domain and peripheral networks. it enforces the DQoSB's admission control decision. The AR resides between the Mobile Terminal and the A3C server in the domain. Therefore, using security terminology, the AR acts as an Authenticator (Auth) with the DA3C server.
- *Mobile Terminal (MT):* The MT is the user's device used to access the network and to request a service. To comply with the heterogeneity of 4G systems, the MT should be able to get the subscribed service using the best available access network.

So what we explained so far is the Y-Comm Framework along with it’s structure so we need to define the threats for this Architecture. AKA was selected as the security protocol.
In order to see the new threats in the network , the author in [3] makes analysis of the AKA of the Mobile Ethernet and then tries to implement it on the Y-Comm Framework to model the Threats that will result from this implementation .
the AKA in the Y-Comm framework have been modeled with 3 layers to comply with Y-Comm Security layers [3] we will be working in the NL-AKA on NAS layer.

The Network-Level AKA (NL-AKA) Protocols:

Achieves mutual authentication Between the mobile terminal and the access network. thus addresses some functions of the Network Architecture Security (NAS) layer. For network level security, two protocols have been defined:

the AKA protocol for the initial authentication process and the AKA protocol for the authentication in case of handover [10].what we will work on in the case of initial Registration .

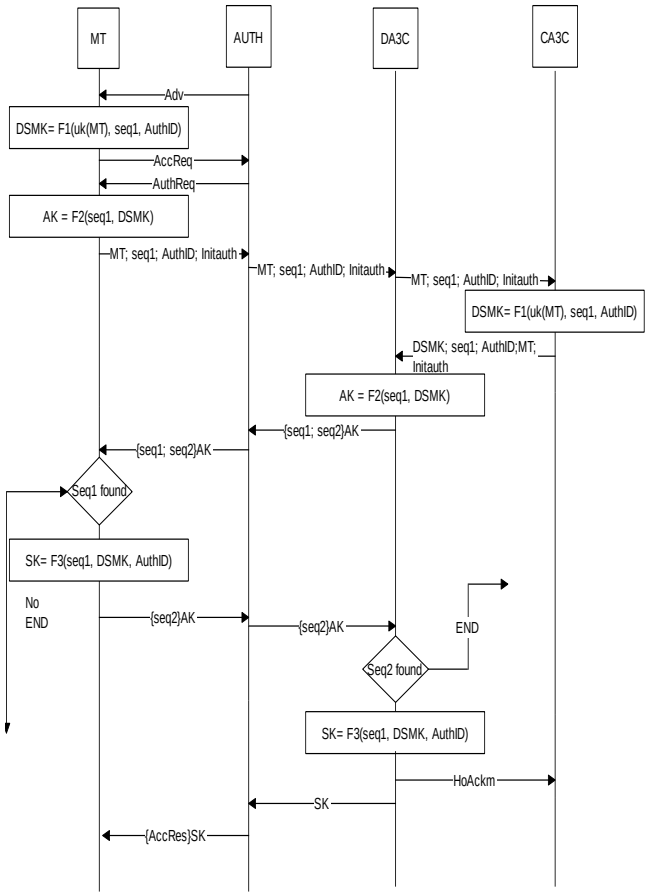


Fig. 3Initial Registeration with NL-AKA

As shown on fig 3 the Model works with the Idea of challenge seq1 and challenge response to MT to verify the User. So first the MT sends to the CA3C (MT,Authid, Intialauth)and from MT Side there are two key formed first is the DMSK and from it AK. Then when the CA3C receive the MT, Authid , it Forms the DMSK Key and sends it to DA3C with Seq1 and Authid. the DA3C forms the AK from DMSK and then generates another sequence seq2 and encrypt it with AK along with seq1 and sends it to MT. The MT confirms the seq1 is there then makes the SK and then the MT reply to DA3C with seq2. The DA3C receive the message encrypted with AK and DA3C ensure that the Seq2 that was received is there.DA3C confirms to CA3C with acknowledge and sends SK to Auth which encrypt acknowledge message to MT.

The Threats that was modeled are

1. Mutual Entity Authentication
2. Mutual Key Authentication
3. Mutual Key Confirmation
4. Key Freshness:
5. Unknown Key Share:
6. Key Compromise

This System was Modeled Using CASPER language and was checked by FDR with the above threats and there was several attacks found from the Model after checking it with Casper/FDR.

So these attacks that found will be described in the next section.

III. PROPOSED WORK

The Mentioned Attacks which can be found in [3] in the verification process with FDR. the author in [3] suggested that there should be Secure channels between Core Nodes CA3C and DA3C and AUTH using IPSEC or VPN. And in reality it is hard to make VPN connection between this huge no of operator and networks. But there should be away of authorization and encrypting the info between the nodes.

This was made on our case by making that the operator already made agreement of which node they authorize by giving them Secure Key connected with the operator this is made between the Auth of the same Domain with DA3C which nodes should be authorized and also between the CA3C and DA3C with the Same Terminology.

the threats model that was actually found from the Unsecure Channels are :

1- The first attack is against the Secret(MT, SK, [Auth, DA3C] assertion. where the Intruder launches a replay attack and eventually manages to get the secret key (SK).Due to insecure communication between DA3C and Auth and the problem solved as the communication is encrypted .

2- The second attack is against authenticity specification Agreement (DA3C, MT, [AK]). In which, the intruder replays messages between the different parties and manages to impersonates the DA3C to the MT. this threat is secured in our model cause the DA3C and CA3C encrypt their data so they can break replay attack.

3- The third attack, is against the WeakAgreement(Auth, DA3C) assertion. The DA3C mistakenly believes it has successfully completed a run of the protocol with the Auth. However, in reality it was running the protocol with Intruder. The threat is secured because

there is Mutual authentication between the parties used so there is no intruder can impersonate one of the parties.

The system that is shown below shows the implementation of authentication and encryption between Core Nodes inside AKA protocol

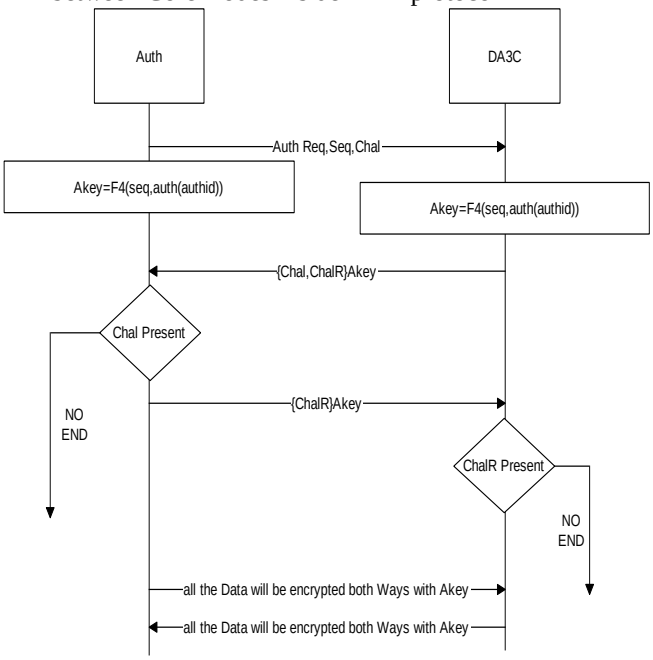


Fig. 4 Authentication and Ciphering Model

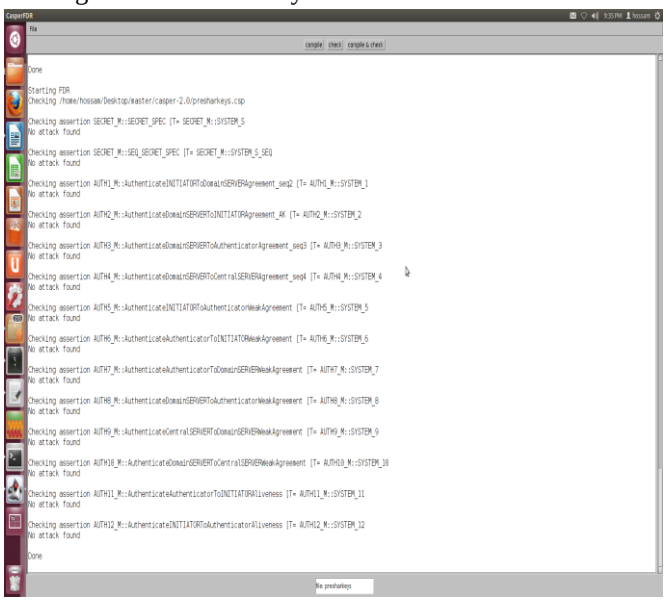
First the Auth sends Auth Req with it's Identity with a challenge and a Sequence generated from the node. DA3C will receive message and make AK and reply with the challenge response Chal,ChalR . Auth will check on the Chal and if found then reply with ChalR and DA3C will check on it.

We Had random generated alphabetic (seq) from Auth along with it's identity and Challenge (Chal) this is sent towards the DA3C server. Auth already had a Hash Function with (seq) and Pre shared key to form a new key generated AK. DA3C uses the same function with the received random Alphabetic (seq) and Had the Pre shared keys to make AK. DA3C replies with challenge response (Chal) along with another challenge (ChalR) encrypted with AK. Auth checks on Chal and if there will reply with ChalR. DA3C checks this Challenge (ChalR) from Auth. This type of authentication is used also between DA3C and CA3C. After the Authentication Process is completed as shown on Fig 4 all date that will be sent will be encrypted after authentication process.

IV. VERFICATION

Verification was made using Casper/FDR for the threats below:

1- Mutual Entity Authentication: There should be a way of the Auth authenticate the DA3C and DA3C authenticate the Auth. There is a Key shared between the Two nodes and the derivation function. the Auth uses the encrypted Chal to make sure that this Is the correct node and also the DA3C Makes the same with challenge ChalR.
2- Mutual Key Authentication: checking was done for DA3C and Auth and DA3C and CA3C attacks using CASPER with secret(DA3C,Auth), secret(DA3C,CA3C). Casper/FDR did not find attacks for this threat .
3- Mutual Key Confirmation: the entities that encrypt the information have the same key. Check was made by CASPER with (Decryptable). this check is made and if it fails the protocol ends.
4- Key Freshness: we include fresh random values in the key derivation of Akey and Dkey with Hash Function. this agreement is made with each new authentication. the new Random values made the Key freshness not violated.
5- Unknown-Key Share : this check was made with Casper by Weakagreement of (DA3C,CA3C), (Auth,DA3C) argument. which checks that the argument B will be running the protocol with Argument A and A only.



This Verification was made with Casper after adding the encryption and Authentication along side with security properties and after checking with Casper/FDR there was no attacks found:

Fig. 5 Verification With Casper/FDR

V. CONCLUSION

Y-comm framework is the future of the heterogeneous networks but it had multiple threats

and attacks from open architecture. This will limit the use of this architecture in the future. Adding the authentication and encryption between Core Nodes solved the main threats that found from insecure communication. Verification with Casper ensured that there were no attacks after securing the channels of core nodes. The verification process ensured also that there were no vulnerabilities found for multiple security properties. This solution will provide the Y-Comm with closer steps for use in the future .

REFERENCES

[1] The Evolved Packet Core http://www.3gpp.org/The-Evolved-Packet-Core Accessed (04-11-2013)

[2] LTE http://www.3gpp.org/LTE Accessed (04-11-2013)

[3] Aiash, Mahdi,. ”An integrated approach to QoS and security in future mobile networks using the Y-Comm framework”. PHD Thesis Middlesex University’s.(March 2012)

[4] M. Aiash, G. Mapp, A. Lasebae, J. Loo, R. Phan , "A Survey of Potential Architectures for Communication in Heterogeneous Networks". The IEEE Wireless Telecommunications Symposium (WTS 2012), April 2012. London, UK.

[5]] K Masahiro, Y Mariko, O Ryoji, K Shinsaku, T Tanaka, Secure service and network framework for mobile ethernet. Wirel Personal Commun 29, 161–190 (2004)

[6] K. Masahiro. APG-Report: “Scalable Mobile Ethernet and Fast Vertical Handover.” IEEE Wireless Communications and Networking Conference (2004)

[7] IEEE 802.21/D8.0. Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services. 2007.

[8] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y. Cheng, A. Dutta, D. Baker, M. Yajnik, D. Famolari. “IEEE 802.21: Media Independent Handover: Features, Applicability, and Realization.” IEEE Standards In Communications AND Networking. (2009).

[9] U. Horn,C. Prehofer, H. Karl. “Ambient Networks - An Architecture for Communication Networks Beyond 3G. IEEE Wireless Communications”. vol. 11, no. 2 (2004).

[10] Mahdi Aiash1, Glenford Mapp1, Aboubaker Lasebae1, Raphael Phan2 and Jonathan Loo1 “A formally verified AKA protocol for vertical handover in heterogeneous environments using Casper/FDR” Eurasip journal on wireless communications and networking (2012). http://jwcn.eurasipjournals.com/content/2012/1/57

[11] Formal Systems, Failures-divergence refinement. fdr2 user manual and tutorial, June 1993, Version 1.3.

[12] M. Aiash, G. Mapp,A. Lasebae. “A QoS framework for Heterogeneous Networking”. .The International Conference of Wireless Networks (2011)

[13] G. Mapp, F. Shaikh, and M. Aiash, R. Vanni, M. Augusto and E. Moreira. “Exploring Efficient Imperative Handover Mechanisms for Heterogeneous Wireless Networks.” International Symposium on Emerging Ubiquitous and Pervasive Systems (EUPS-09), 2009.

[14] G. Mapp, F. Shaikh, D. Cottingham, J. Crowcroft, J. Beliosian. “YComm: A Global Architecture for Heterogeneous Networking”.3rd Annual International Wireless Internet Conference (WICON 2007), 2007.

[15] G. Lowe, P. Broadfoot, C. Dilloway, and M. L. Hui, “Casper: A compiler for the analysis of security protocols”, http://www.cs.ox.ac.uk/people/gavin.lowe/Security/Casper/index.html 2.0 ed., Accessed (01-11-2013)

[16] M. Goldsmith G. Lowe A.W Roscoe P. Ryan, S. Schneider,” The modeling and analysis of security protocols”, PEARSON Ltd, 2010.

[17] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, and S. Shenker. “Off by Default!” In ACM HotNets, 2005