

Evaluating Techniques for Network Layer Independence in Cognitive Networks

Muthukumaran Pitchaimani, Benjamin J. Ewy, Joseph B. Evans
Information & Telecommunication Technology Center
University of Kansas
Lawrence, KS 66045 USA

Abstract— Cognitive networks are the latest progression of cognitive functionality into the networking stack, an effort which began with a layer one and two focus on cognitive radios, and has lately been extended to layer three and beyond. In this paper we evaluate an approach to network layer independence in wireless cognitive networks, utilizing and extending HIP to provide host identity across a myriad of network layers that evolve to meet application and environmental constraints and requirements. We detail a use case for this type of flexibility, specifically, a disaster relief scenario with complex usage and security requirements, and present evaluations that validate this approach. This work is a part of CogNet, an architectural framework for research into architectural tradeoffs and protocol design approaches for cognitive radio networks at both local network and the global internetwork levels.

I. INTRODUCTION

We are now all too familiar with the threat and impact of large-scale natural and human caused disasters on society. A defining characteristic of many disasters is that there is a desperate and immediate need for information so that the impacted can react as appropriately as possible (e.g., leave a location or stay put), so that first responders can communicate with victims and each other, and so that authorities can coordinate overall response efforts. An emergency network formed for such a situation must (1) handle flexible communication needs under extreme conditions, (2) offer organized control and management of the involved network assets, (3) provide robust support to a wide variety of critical services, and (4) provide secured and at the same time assured access to these services and assets.

Existing communication systems like the cellular network struggle due to infrastructure reliability in these conditions and their fixed band operation. Further, many existing communication systems lack data transfer capabilities which are crucial in emergency situations with inherent disparate contextual messaging needs. Emergency networks need dynamic access to RF spectrum to meet the rapidly changing communication requirements and widely differing RF environments.

Cognitive radios [1][2] and networks formed using these techniques promise to offer the capabilities to suit these

requirements. In a disaster response scenario, relief efforts use ad-hoc techniques extensively. The defining characteristic of these situations is the need to establish a quick communication infrastructure without a well thought out plan for connectivity but with a need for robust capability to form and dismantle networks in a highly dynamic way. While wireless communication in various spectrum bands is indispensable in the relief effort, the radio spectrum is perceived to be scarce because of inflexible allocations. There is a need for quick adaptation to available bands for urgent communication e.g. distress call. Cognitive radios offer the requisite agility in employing dynamic spectrum selection by rapidly adapting itself to changes in spectral usage with interoperability among multiple interface standards.

The network layer protocols for such cognitive radio networks are still in the nascent stages of development. In order to effectively exploit the latent capabilities of these cognitive radios in disaster response and other multi application mobile environments, we propose a new hierarchical multi-overlay approach to address effectively the required application robustness and security. The networking assets involved in forming such a network will be owned by disparate entities during deployment spread across different geographical locations spanning multiple policy domains adding further complexity.

The extension of cognitive radio capabilities to the network layer, providing multiple network services within a framework supporting mobility, and providing a security framework for accessing these services are key components in providing solutions to demanding networking environments such as disaster relief.

The remainder of this paper presents the architectural context for this work, a cognitive networking layer approach, experimental results, and some conclusions.

II. COGNITIVE NETWORK PROTOCOL STACK BACKGROUND

A. Architectural Context and Framework

The approach to cognitive networking described in this paper fits within a broader architectural context. In order to support cognitive networking capabilities, an architecture needs to offer views into the protocol elements to provide information for the sensing and learning portions of the cognitive process. To act upon cognitive decisions, the protocol elements must also provide control interfaces. These measurement and control interfaces should be available throughout the protocol stack to enable flexibility at the lower and upper layers.

A cognitive network needs flexibility within and spanning layers [16]. Some of the lower-layer capabilities include a flexible physical layer supporting waveform and coding agility, spectrum sensing and coordination protocols, bootstrapping and topology discovery mechanisms to build a network from a collection of nodes, and media access protocols in accord with the rest of the dynamic and adaptive system.

In order to coordinate and manage a cognitive wireless network, we envision a Global Control Plane (GCP) [3][4], providing cross-layer and cross-network management and control capabilities. The GCP provides these functions not only to a local subnet, but across wireless subnets and the global internetwork. Information on upper layer needs and requirements that are derived from the use case and applications, lower-layer capabilities and environmental conditions, and network node status and topology will be shared and mediated by the GCP. While [3] provides an insight into the overall architecture of GCP, [4] provides a more thorough treatment. Cognitive choices on the selection of network layers will be made and shared throughout the network, in order to meet the challenges of the wireless networking environment.

B. Wireless Networking Challenges

Wireless networking is even more challenging than traditional fixed networking for several reasons. First, mobility is inherent with untethered devices, and this imposes demanding architectural requirements for naming, localization, addressing, and routing. Second, resources are constrained because of spectrum “scarcity”, which leads to performance (e.g., bandwidth and delay) issues. Third, because of mobility, the operating environment for a wireless device will change as the node changes its surroundings (e.g., between indoor, urban, or rural). Fourth, the physical properties of the wireless communications path change over time and result in the possibility for rapid topological transformations at the network layer [5].

Cognitive networking techniques promise to address the challenges arising from wireless communications.

III. COGNITIVE NETWORK LAYER

A. Architecture and Requirements

To provide the services required for complex usage scenarios such as disaster relief support, the cognitive network layer needs to support a variety of applications including data and mobile real-time services (e.g., voice). To enable these applications given the variability of wireless communication, the CogNet framework provides a cognitive, multi-overlay network layer that can adapt based on sensing and learning of the cross layer environment, the communication model for the applications (e.g., one-to-one, one-to-many), and policy and security constraints. The latter issues of policy and security are particularly important in a cognitive radio environment where opportunistic communications with previously unknown nodes may become common, and comprise the focus of this work.

Our cognitive network layer provides both the traditional IP network layer and non-traditional overlay-based mechanisms for communication within a subnet. Routers serve as a gateway between local network layers within the cognitive network as well as to the Internet. Overlays provide a large

number of optimization points, and may be tailored to the application at hand. This allows us to provide multiple network layers tailored to specific applications or communication flow types. Examples include routing overlays which have shown promise in ad hoc network layer routing scenarios [6], and application tailored overlay structures such as topologically aware overlays for group messaging applications [7]. Fig. 1 illustrates a cognitive radio network with mobile nodes and an interconnection to the wired core network through a router aware of the cognitive local subnets. Use of a particular overlay will be decided upon by cognitive techniques (e.g., case-based reasoning, machine learning) based on factors including the wireless environment, application, and policy. Such cognitive decisions are similar in nature to decisions made at layer 2 [16], and the application of particular methods to the networking layer is being investigated. In our example, Overlay 1 could be an IP network layer, while Overlay 2 could be a multicast optimized DHT-based network layer being used to support a messaging application.

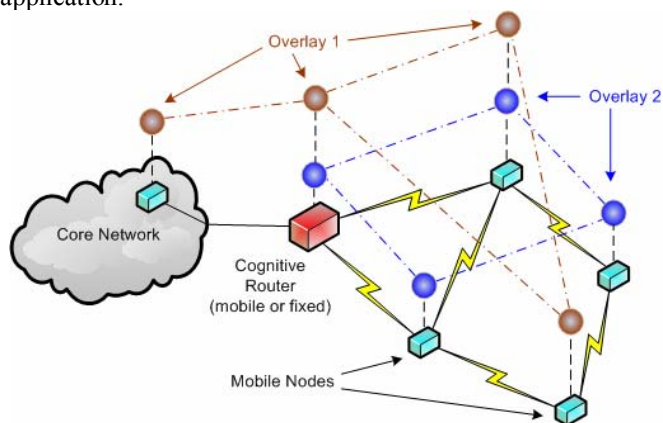


Figure 1. Cognitive wireless network with multiple network-layer overlays

A cognitive network layer needs naming and addressing mechanisms that provide for self-organization, translation for global reachability, and merging / disconnection of cognitive networks themselves as well as with the wired network infrastructure. One important requirement is the decoupling of end point identity from any topological addressing, particularly in the mobile environment.

B. Host Identity Protocol for Mobility

IP as a network layer typically provides two roles, location identity and end-point or host identity. The use of IP for both tasks has complicated mobility solutions [8] [9] [10], and resulted in various extensions to overcome this fundamental constraint. Host identity protocol (HIP) [11] cleanly separates this functionality by leaving location identity to IP and introducing a new name space based on *host identifiers*. This name space is inserted between the network and transport layers, allowing the transport layer to bind persistent host identities that can migrate among locations (and their corresponding IP addresses) so that higher layers can transparently function across the mobile environment. While HIP is intended for use in both non-mobile and mobile environments, for the purpose of this work we focus on its application in the mobile environment.

Host Identifiers are the public keys from a public-private key pair, and the public portion can be published using

mechanisms such as DNS. In order to allow flexibility in the public-private encryption algorithms used, the host identifier is subjected to a 128 bit hash to create a *host identifier tag* (HIT) which is exchanged between hosts using a Diffie-Hellman [12] based mechanism to provide authentication of the end points. The HIT is then used by the transport layer to bind sessions to host identities instead of the IP address, decoupling the host's identity from its location.

HIP has been extended [13] to provide LOCATOR records that allow a host to notify its peers about an IP address change, allowing for session preservation as a host moves from one IP address space (location) to another. This method is intended for hosts that are already communicating, i.e. have completed the HIP base exchange. For hosts trying to start a new session, with one or more operating in a changing IP environment, further extensions [14] provide a Rendezvous (RVS) Server. Using RVS, a host will register its HIT and current IP with the RVS, and publish its HIT and the RVS's IP address (which is presumed to be largely fixed) into DNS. When a host wants to initiate a session with the mobile host, it will send its initial packets to the RVS which will then relay them to the current IP address of the destination host. The mobile host updates the RVS as it moves from one location to another. This allows two hosts who have not communicated to create sessions in a mobile environment.

C. Extending HIP for Multiple Layer 3s

Initial proposals of HIP were geared towards providing network address independence primarily in multihoming and mobility situations within a single namespace with upper layer states maintained with host identity. This is achieved using the "readdress" packet handoff by a host that relocates itself to a new network address. We propose to use this readdress mechanism to send address and associated information for a new namespace. Currently it is assumed that the cognitive nodes participating are capable of adapting to multiple network layers known to the system. This multi-homed assumption provides a simple prototype model that avoids the use of a protocol gateway for network layer-layer translation. The transition to a new network layer that is selected as optimal for a particular communication (either by cognition, mobility or otherwise) involves readdressing into the new layer's address space. This can be achieved by a node updating its availability in the new address space to their peers, optionally updating the corresponding RVS server. We believe HIP provides sufficient infrastructure to provide network layer adaptation with little cost.

D. Security Model for Cognitive Layer 3s

The key based identity provided by HIP enables various security functions like authentication, confidentiality, and integrity. The HIT can be used not only for end point sockets but also as a handle for encryption and for specifying authorization information. Specifically, every readdress message is followed by a "cookie challenge" which the node issuing the message should use to authenticate itself. This authentication mechanism can be opportunistically used for security functions outside of HIP for example, authentication in access control mechanisms. This can be provided by using an access control mechanism within a policy framework that provides a general platform for policy expression and

enforcement at different levels. Within this, the restrictions to a network layer are specified using admission control policies so that only authorized nodes become member of protected network layers. Unauthorized nodes are either rate limited or disallowed depending on the policies of the network layer. The framework provides sufficient granularity to pass on delegation to an identity representing an individual or group of nodes. KeyNote [15] is a system with unified notions of security policy, credentials, access control, and authorization. It provides a common domain independent assertion language that has flexible mechanisms to represent wide variety of security specifications.

KeyNote provides various abstractions to represent entities to which authorization is delegated. These are sources of actions that need to be controlled. The principals are identified by the Host identities (HITs) or names to identify roles. The attribute value set is a common provision to describe actions and policy conditions. A logic engine answers the queries of compliance with application specified value.

Within our CogNet framework we restrict access to various layer 3 network layers by checking for compliance using KeyNote against the implemented policies. For example the 'join' action that is performed by the node to access a particular layer 3 network is checked against admission control policies. Additionally, nodes that can perform special actions are required to present the authorization information during the request for that operation, such as a relief unit requesting access to a video sensor in a private building. This authorization information must be obtained before hand and certified by a delegation authority such as a management overlay or a service of the GCP.

E. Dynamic Layer 3 Selection

The routing decision made by cognitive radio nodes is based upon information learned from various sections of the environment like communication needs at the application level, security constraints and lower layer states like link quality etc. We propose extending work done [16] for L1 and L2, to account for the L3 selection, and create an optimized solution for the combination of layers. This encompasses a decision making involving both the selection of appropriate network layer and routing decisions within the selected layer. The dynamic nature of the delay associated with the decision making algorithm required to switch to an alternate network layer raises various issues of naming and state maintenance. In HIP there is a natural state maintenance by associating higher layer associations with the host identifier. Hosts then assume the responsibility of disseminating updates about its new location identifier. This can be exploited to provide information about the network layer changes and associated name material distribution. The hosts then utilize the more appropriate network layer without affecting higher layer states. In particular the LOCATOR information in the update message can be utilized to inform the peer about the associated changes. We assume here all the cognitive nodes are able to identify and participate in the desired network layer.

IV. RESULTS

A. A Disaster Relief Scenario

We evaluate the utility of a cognitive network layer and our proposed security model in the context of an example scenario with four different environments in a hurricane relief effort, illustrated in Fig. 2.

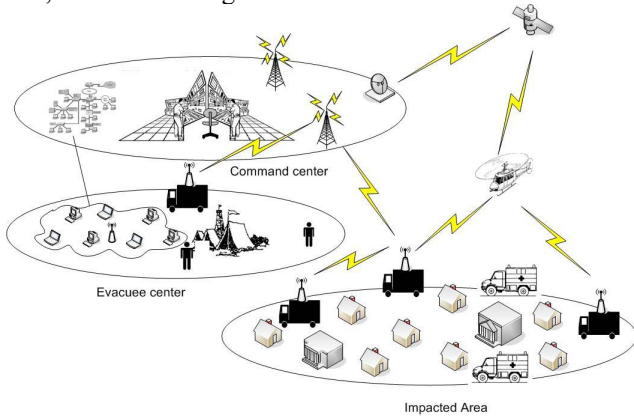


Figure 2. A disaster relief scenario

- i. *A Command Center*: This center controls and co-ordinates the relief effort forming a headquarters for relief efforts. It houses several critical services essential during the operation and is expected to have high speed wired network connectivity. It also provides wireless connectivity geared towards rapid growth and will utilize these wired and wireless systems to receive updates from the impacted area on needs, available routes, local conditions etc, and then coordinate the delivery of supplies via a relief tracking center, and the initiation of rescue missions based on information received from the Impacted Area (broadcasts for help) or specific leads provided by people at the Evacuee Center. This forms the epicenter of all the one-one and one-many services provided and such must be secured against network problems due to either deliberate or overuse based denial of service problems.
- ii. *An Impacted Area*: This is the actual affected area connectivity is primarily provided by wireless units deployed after the incident. It will have multiple wireless subnets and be the target for point to multipoint announcements, and point to point coordination with privacy requirements.
- iii. *An Evacuee Center*: This area serves as housing for those displaced by the emergency. It is a rapidly growing center which will utilize cognitive radios' to provide coverage and access to a growing population, expected communication flows of broadcasts (finding relatives) and point to point communications (requesting supplies etc), and will transition to a more traditional mix as the center works to provide longer term communication needs (telecommunicating, etc.) Users from this growing set need to be authenticated as belonging to the Evacuee center before they are provided with the services of the command center.
- iv. *A Relief Relay Center*: This is a quickly deployed center with mix of wired and wireless to catalog and direct relief. It will utilize wired and wireless capabilities with

mobile scanning and tracking devices (RFID, etc) to catalogue shipments of supplies, and provide directions to get the supplies to the area where they are needed most.

B. Service Requirements in this Scenario

Each center has its own messaging requirements and applications which together with varied need for security gives rise to set of needs an emergency setup should meet

- *Connection Persistence*: Response scenarios typically involve high node movements often across various realms. Such mobility should not impede ongoing sessions especially during relief relay operation.
- *Traffic pre-emption*: Network infrastructure deployed during emergency scenario is shared among many disparate entities. However there should be provision for prioritizing among traffic to support critical emergency communication and a flexible way to specify and enforce preemption policies.
- *Robust churn support*: Emergency network should cope with rapid change in node memberships and be robust against unpredictable topology changes.
- *Communication isolation*: A support for protection of various communication classes among different centers through privacy and isolation providing multiple simultaneous private channels.
- *Authentication and authorization*: The cryptographic functions provide for authentication of nodes or a group of nodes that are authorized to perform privileged operations. For example the nodes that are authenticated to belong to a management overlay can request for sensor data in the impacted area.

C. Experiments

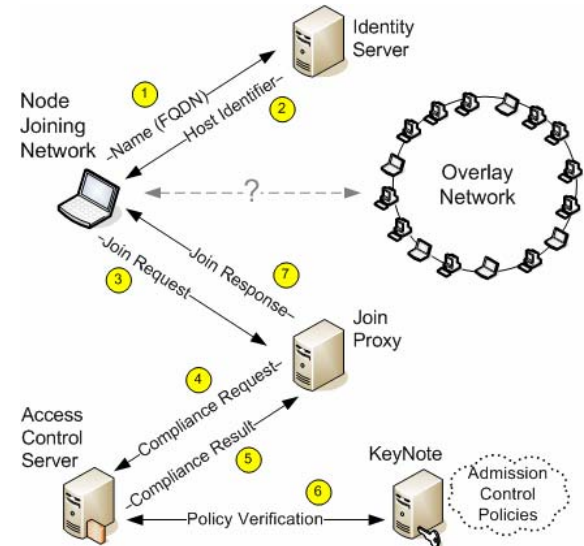


Figure 3. Node joining overlay network in testbed

We developed an experimental testbed (Fig. 3) that allows us to evaluate the effect of introducing alternate network layers, as well as the impact of utilizing policy to enforce access to these network layers. The introduction of delay into connection setup was explored because this architecture introduces three components of delay to a typical network stack, mobility induced (HIP), network layer selection, and

security policy lookup and enforcement. The network layer selection delay is a function of the algorithm used, and the focus of ongoing work. In these experiments we focused on the delay induced by adding mobility indirection (HIP) and the security policy framework introduction to the network layer setup.

We utilized a Chord [17] overlay as a model for an alternate network layer, and varied the average number of nodes from 2 to 32 and observed the delay induced due to the policy framework within our stack. For example we ran the experiment on 16 nodes with one node playing the part of the access control server which is consulted for policy compliance. The experiment was repeated with simultaneously many nodes leaving and joining the system with the average node population maintained as approximately a constant. These policies, including the node identifiers, were implemented in KeyNote. As each node joins into an overlay, a request is sent to the access control server. The server checks the compliance of the join against existing policies for node admissions. On successful compliance the joining node is supplied with the required overlay information. These actions correspond to steps 3-7 in Fig. 3; the delays found are presented in Fig. 4 This same setup was also used to represent node capabilities for various messaging options inside the overlay. To test the delay induced due to the policy compliance mechanism and test the response of this setup to scalability especially for rapidly changing environment such as in the evacuee center, the expectation is that the policy framework induces a roughly constant delay even with simultaneous node joins and leaves and with an average number of total nodes participating in the overlay at any given point of time. It was observed in Fig. 4 that our framework did have a roughly constant response time. Fig. 5 summarizes the delay induced due to additional mobility indirection. The penalty incurred due to this component was found to be negligible on normal message exchange scales.

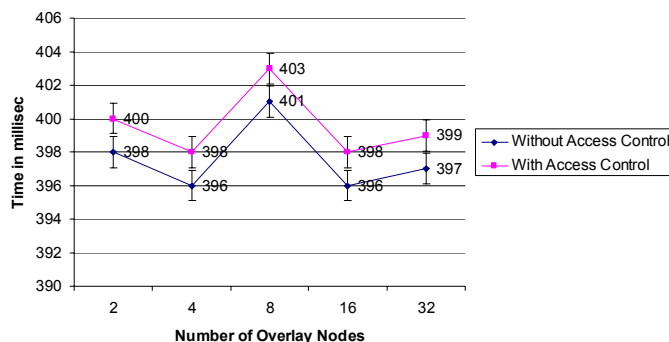


Figure 4. Experimental results – delay to authenticate and join the overlay

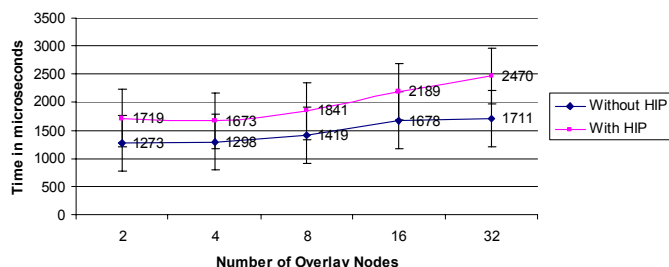


Figure 5. Experimental results – delay due to HIP

V. CONCLUSIONS

This paper has described a cognitive networking approach for addressing the challenges of the emergency response environment. Building upon HIP and Keynote, this approach provides improved support for mobility as well as security, and offers flexibility at the network layer. Experimental results show that the impact of indirection and trust management services is minimal. These architectural innovations promise to form a foundation for cognitive adaptation of network layers.

REFERENCES

- [1] J. Mitola III. *Cognitive Radio: An Integrated Agent Architecture for Software Radio*, PhD thesis, Royal Institute of Technology (KTH), Sweden, May 2000.
- [2] FCC 03-322 NPRM on Cognitive Radio, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-322A1.pdf.
- [3] D. Raychaudhuri, N. Mandayam, J. B. Evans, B. J. Ewy, S. Seshan, P. Steenkiste, "CogNet - An Architecture for Experimental Cognitive Radio Networks within the Future Internet", 1st ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture (MobiArch 2006), San Francisco, December 1, 2006.
- [4] J. Xiangpeng, D. Raychaudhuri. "Global Control Plane Architecture for Cognitive Radio Networks". to appear at IEEE CogNet 2007. Glasgow, Scotland, June 2007.
- [5] P. Marshall, private communications.
- [6] M. Caesar, M. Castro, E. Nightingale, G. O'Shea, A. Rowstron, "Virtual ring routing: network routing inspired by DHTs," SIGCOMM Comput. Commun. Rev. 36, 4 (Aug. 2006), 351-362.
- [7] M. Castro, P. Druschel, A-M. Kermerrec and A. Rowstron, "SCRIBE: A large-scale and decentralised application-level multicast infrastructure", IEEE Journal on Selected Areas in Communication (JSAC), Vol. 20, No. 8, October 2002.
- [8] A. Snoeren and H. Balakrishnan, "An End-to-End Approach to Host Mobility", Proceedings of ACM Mobicom Conference, 2000.
- [9] C. Perkins et al., "IP Mobility Support" Internet Request For Comments (RFC) 2002, October 1996.
- [10] C. Perkins et al., "IP Mobility Support for IPv4" Internet Request For Comments (RFC) 3344, August 2002.
- [11] R. Moscowitz, "Host Identity Payload and Protocol", Internet Draft: draft-moscowitz-hip-05.txt (work in progress), November 2001. Available online at <http://homebase.htt-consult.com/HIP.html>.
- [12] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. Info. Theory IT-22, 644-654, November 1976.
- [13] Internet-Draft draft-ietf-hip-mm-04 June 23, 2006 Internet Engineering Task Force Expires: December 25, 2006 Network Working Group.
- [14] Internet-Draft draft-ietf-hip-rvs-05 June 7, 2006 Internet Engineering Task Force Expires: December 9, 2006 Network Working Group.
- [15] Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. "KeyNote: Trust management for public-key infrastructures" (position paper). Lecture Notes in Computer Science, 1550:59--63, 1999.
- [16] T. Newman, B. Barker, A. M. Wyglinski, A. Agah, J. B. Evans, G. J. Minden, "Cognitive Engine Implementation for Wireless Multicarrier Transceivers", to appear in Wiley Wireless Communications and Mobile Computing, 2007.
- [17] I. Stoica, R. Morris, D. Karger, M. Kaashoek, and H. Balakrishnan. "Chord: A scalable peer-to-peer lookup service for internet applications", in Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications, 149-160.