Proceedings

ExtremeCom 2011

3rd Extreme Conference on Comunication
The Amazon Expedition, Brazil

September 26-30, 2011

Manaus, Brazil

in co-operation with ACM / SIGCOMM

acm In-Cooperation

in co-promotion with SBC / CAPES

SBC CAPES

Sponsored by
Faber-Castell, FUCAPI, INPA, INRIA, and SEMMAS

FABER-CASTELL FUCAPI INPA

inria informatics mathematics SEMMAS

Work in Progress: Towards an Architecture for Managing Delay-Tolerant Emergency Networks[*]

Ewerton M. Salvador
Universidade Federal de Minas Gerais
Dept. of Computer Science
Belo Horizonte, MG – Brazil
ewerton@dcc.ufmg.br

Daniel F. Macedo
Universidade Federal de Minas Gerais
Dept. of Computer Science
Belo Horizonte, MG – Brazil
damacedo@dcc.ufmg.br

José Marcos Nogueira
Universidade Federal de Minas Gerais
Dept. of Computer Science
Belo Horizonte, MG – Brazil
jmarcos@dcc.ufmg.br

Jéferson C. Nobre
Universidade Federal do Rio Grande do Sul
Institute of Informatics – II
Porto Alegre, RS – Brazil
jcnobre@inf.ufrgs.br

Pedro A. P. R. Duarte
Universidade Federal do Rio Grande do Sul
Institute of Informatics – II
Porto Alegre, RS – Brazil
paprduarte@inf.ufrgs.br

Lisandro Z. Granville
Universidade Federal do Rio Grande do Sul
Institute of Informatics – II
Porto Alegre, RS – Brazil
granville@inf.ufrgs.br

ABSTRACT

Delay-Tolerant Networks (DTNs), just like any other computer network, need to be managed. However, until now little was achieved in the research for specific management solutions for DTNs, due to the fact that these networks are still in their infancy. In this paper we present some initial steps in the development of a management architecture for Delay-Tolerant Emergency Networks (DTENs), which is a specific case of DTN. Among the design definitions of our architecture, we can cite the use of the policy continuum concept, the division of the network into groups and the need for autonomic control loops to implement local management functions.

1. INTRODUCTION

When a certain region faces a disaster situation, it is common that its telecommunication infrastructure is lost. In order to coordinate the efforts for mitigating the emergency, communication and coordination among the rescue teams is essential. It is desirable that the people working in an emergency scenario make use of mobile devices that connect themselves using wireless network interfaces. This way, the range of information supports available for aiding the disaster mitigation efforts might be improved with resources such as interactive maps, real-time images and videos, among others [2]. However, some factors may break the network connectivity in this kind of scenario, such as: natural obstacles, wreckages, limited transmission radius of the mobile devices, etc. Because of disconnections are a common problem in these networks, the use of a delay-tolerant architecture [3], forming a Delay-Tolerant Emergency Network (DTEN), allows the use of mobile computing devices in disaster environments.

The use of a management solution is of great importance for any type of network, including DTNs, in order to maintain its devices operational and to keep up with the standards defined in a Service Level Agreement. However, it is very unlikely that traditional management solutions will work properly in DTNs, since they are based in some assumptions that are broken in these networks, such as low delay data exchange and permanent connectivity. In this paper we describe our initial steps in the development of a Delay-Tolerant Network Management (DTNM) solution suitable for an emergency scenario.

2. AN ARCHITECTURE FOR DELAY-TOLERANT EMERGENCY NETWORKS

A DTEN will use delay-tolerant communication capabilities for overcoming constant link disconnections and long propagation delays. In such networks, the nodes are composed of a diversity of mobile devices (smartphones, laptops, palmtops, etc.), operated by the people working in the emergency scenario. These people form teams, and each team has a local coordinator (manager). These coordinators, in their turn, are administrated by a Central Management Entity that manages the entire region operations. Regarding this central entity, we assume that it employs devices with more powerful computational and communication capabilities, when compared to the equipment used by the rescue teams. However, the transmission range of this central entity is also limited, and remote communication with the rescue teams will be necessary.

A mechanism that allows a node inside a group to monitor itself and its neighbors is being designed. Since the occurrence of faults in the DTENs has the potential of compromising the entire rescue operation, **fault management** was chosen as the first priority in our DTEN management

[*]The authors would like to thank CNPq, CAPES and FAPEMIG, brazilian research agencies, for their financial support in this work.

ExtremeCom2011, September 26-30, 2011, Manaus, Brazil.
Copyright 2011 ACM XXX-X-XXXX-XXXX-X/11/09 ...$10.00.

solution. Our second priority in the development of the proposed architecture is **configuration management**, since the time to prepare nodes rescue operations is another critical aspect of our scenario. Once the network operator defines the desirable network behavior, in a high-level fashion, it will be translated in configuration commands by the DTNM architecture, and then these commands will be deployed in the devices. In fact, this process may occur when the network is already deployed in the disaster scenario, with new configuration messages being sent remotely, via the Bundle protocol. **Performance management** and **accounting management** will be executed mostly inside the groups of nodes. By doing so, we attempt to take maximum advantage of the local communications in acquiring up-to-date information, since we are free of the restrictions imposed by the use of the Bundle protocol. Finally, **security management** has fundamental importance since the privacy, authenticity and integrity of the data shared among the mobile devices is essential in emergency networks. Solutions for the problems faced in security management are still being studied.

2.1 Local and Remote Management

Every time two or more nodes are inside the transmission radius of each other, they form a local group [1] [4]. Each group has at least one local manager. This manager gathers information from its neighbors and from itself, autonomically, via periodic polling, without the need of using the Bundle Protocol. Because of the cost of this polling process, only a small quantity of essential parameters should be monitored in order to avoid excessive bandwidth usage. If any problem is detected during the polling process, the local manager can start the proper fault correction routines without the intervention of the Central Management Entity.

Local groups are organized dynamically. Moreover, various groups can be merged into one single group. However, events in the disaster region may lead to a group being divided into two or more groups. Because of this, the local manager has to be chosen dynamically, and some sort of voting mechanism should be employed for selecting the group's manager(s). The election mechanism shall be periodically in order to verify if it is necessary to redefine the group and choosing new managers. This mechanism also has to take into account the capabilities (processing, energy, secondary storage, link usage, etc.) of the local manager to ensure that they are not above a pre-determined threshold, which would indicate an overload. In fact, voting mechanisms for selecting local managers were studied in ad hoc networks, and it is possible that these mechanisms can be employed in our DTNM with some adaptations. We are currently investigating such mechanisms.

The remote management capabilities of our DTNM architecture are invoked when a group of nodes needs to communicate with the Central Management Entity, or vice-versa. This communication must be performed through the use of the Bundle Protocol in order to overcome disconnections and long delays that are likely to occur in these emergency environments. By doing so, we are attempting to minimize the use of remote communication in the DTEN.

2.2 Policy Continuum

The *policy continuum* concept was proposed by John Strassner [5]. A popular approach to manage networks is the utilization of policies, which defines a Policy-Based Network Management (PBNM) architecture. Strassner proposed a multi-level architecture for PBNM systems, where the highest levels are concerned with the management of the network at a very abstract, business-driven level, while the lowest levels are concerned with device-specific issues. Each level i will derive its policies based on the policies defined on level $i + 1$. Hence, the policies on any given level of the policy continuum are essentially the refinement of the policies found on the levels above it. This architecture is suitable for self-managed networks, which is the case of our DTEN, since it assumes that humans will only intervene over the highest level, by setting the service-level agreements (SLAs) and high level goals of the network. The number of levels will depend on the complexity and/or the needs of the managed network. One of the challenges of the policy continuum lies in the identification of the number of levels to be implemented and their level of abstraction, which is being studied at the present moment.

3. CONCLUSIONS AND FUTURE WORK

This paper presented some initial considerations concerning the design of a management architecture for Delay-Tolerant Emergency Networks (DTENs). We described how each management functional area defined in FCAPS (Fault, Configuration, Accounting, Performance, Security) model will be contemplated in our proposed architecture. We provided an overview of the functions that will be executed in the local management scope of the proposed architecture, as well as the communication involved in the remote management of a DTEN.

As for future work, we intend to refine various aspects of our architecture, such as: the mechanism for electing managers in a group of nodes, how we will implement security management in our solution and how we will structure the *Policy Continuum* model in DTENs. We will also implement this architecture in a testbed, in order to validate its efficiency and efficacy.

4. ADDITIONAL AUTHORS

Additional authors: Liane M. R. Tarouco (Universidade Federal do Rio Grande do Sul, email: `liane@inf.ufrgs.br`)

5. REFERENCES

[1] E. Birrane and R. G. Cole. Management of Disruption-Tolerant Networks: A Systems Engineering Approach. In *Proceedings of the SpaceOps 2010 Conference, Alabama, United States. April 2010*, 2010.

[2] G. Calarco and M. Casoni. Virtual networks and software router approach for wireless emergency networks design. In *Proc. of IEEE 73rd Vehicular Technology Conference 2011*, 2011.

[3] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss. Delay-tolerant networking architecture. RFC 4838 (Informational), April 2007.

[4] W. Ivansic. DTN network management requirements. Internet Draft (Informational), June 2009.

[5] J. Strassner. *Policy-Based Network Management.* Morgan Kaufmann, 2003.