A Secure DTN-based Smart Camera Surveillance System

Andreas Papalambrou, Panagiotis Soufrilas
Department of Electrical and Computer Engineering
University of Patras
Patras, GR-26504, Greece
+306972154351
papalambrou@ieee.org, ee6373@upnet.gr

Artemios G. Voyiatzis, Dimitrios N. Serpanos
Industrial Systems Institute/Athena RC
Patras Science Park building
Platani, Patras, GR-26504, Greece
+302610910301
{bogart,serpanos}@isi.gr

ABSTRACT

A smart camera surveillance system operating over a DTN network is presented. Low power embedded systems with connected smart cameras are used to detect and record events using motion and other triggers. Smart camera nodes can cooperate by means of a wireless personal area network. Images of events chosen by smart cameras are saved locally and transmitted via a base station node by means of a secure Delay Tolerant Network based on the Bundle protocol with implemented monitoring mechanisms. This network architecture is appropriate for surveillance of remote areas where connectivity is intermittent or frequently disrupted and events are relatively few. In this work, we evaluate the performance of the system, focusing on the communication over the DTN network in order to assess how such a network performs in various scenarios of events and availability, with or without security, and in comparison to existing communication methods.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General – *Data communications, Security and protections*

General Terms

Performance, Security.

Keywords

Delay Tolerant Networking, Security, Smart cameras

1. INTRODUCTION

Smart cameras are used extensively in surveillance applications where human monitoring is difficult or impossible [1]. Typically, most smart cameras are used in real-time applications in order to automatically detect events and notify via an appropriate network infrastructure. However, some surveillance applications need to be carried out in remote areas where terrestrial network infrastructure is often non-existent and other options are difficult or expensive to implement. A solution for network connectivity in such environments is often the Delay/Disruption Tolerant Networking (DTN) [2]. DTN networks are based on specially designed protocols that deal with the unusual communication conditions, such as transmission delays of minutes or hours, intermittent connectivity, and low reliability. In such conditions, typical Internet protocols fail to operate thus, DTN protocols are used either replacing Internet protocols or in conjunction with them. Two of the most studied protocols are the Bundle protocol (BP) [3] and the Licklider transmission protocol [4]. Most work on these protocols is carried out by the Delay-Tolerant Networking Research Group (DTNRG) [5] of the Internet Research Task Force. The Bundle protocol, used in this work, provides DTN networking in addition to convergence layers and cooperation with other protocols. The bundle as the basic packet of information is the central idea behind the Bundle protocol. Nodes, called Bundle Agents, exchange Bundles that consist of various header, payload, and, optionally, security blocks. Bundles are essentially stored and forwarded between nodes when connectivity exists and all mechanisms of the protocol are specially designed to deal with issues that arise when connectivity is interminant. The Bundle protocol received RFC status in 2007 and its security mechanisms in 2011.

No work exists that has studied the use of smart cameras over a DTN network. Since a common field for DTN networks is satellite communications, the DTN networks have been used to transfer data such as photographs and video from satellites [6]. However, the work reported in this paper is focused on specific application requirements of smart cameras for terrestrial environments.

2. ARCHITECTURE OF THE SYSTEM

2.1 Architectural overview and requirements

The proposed architecture of the system extends the use of smart cameras to applications of surveillance in remote areas or areas with poor connectivity. Examples include rural areas, border crossings, isolated islands, or mountainous regions. Connectivity in such areas can be interminant, for instance data collecting vehicles may pass by the area at regular intervals or satellite links may be established at some time frame but not be always available.

The requirements that a surveillance system must meet under these circumstances are the following:

- Distributed processing
- Low power consumption
- Secure operation
- In-network storage availability to account for intermittent connectivity

In order to account for both the surveillance task as well as the communication task, the proposed system needs to be split in two parts that involve the cooperation of two different network architectures. Regarding the surveillance task, the proposed architecture is a distributed sensor network which includes ad-hoc communication between smart camera motes. The communication task

WESS'11, October 09 - 14 2011, Taipei, Taiwan

with the outside world involves the architecure of a Delay Tolerant Network.

2.2 Testbed description

The test system that was used to experiment with the proposed architecture consists of three smart camera motes that make up the distributed wireless sensor network, and an embedded Linux system that acts as a storage unit and is capable of running a DTN stack. Therefore, this system runs as the gateway of the surveillance system to the DTN network and therefore the outside world. The DTN network was set up at the University of Patras and provides not only connectivity between internal nodes but also access to the Internet, including a similar testbed available at the Industrial Systems Institute/Athena RC.

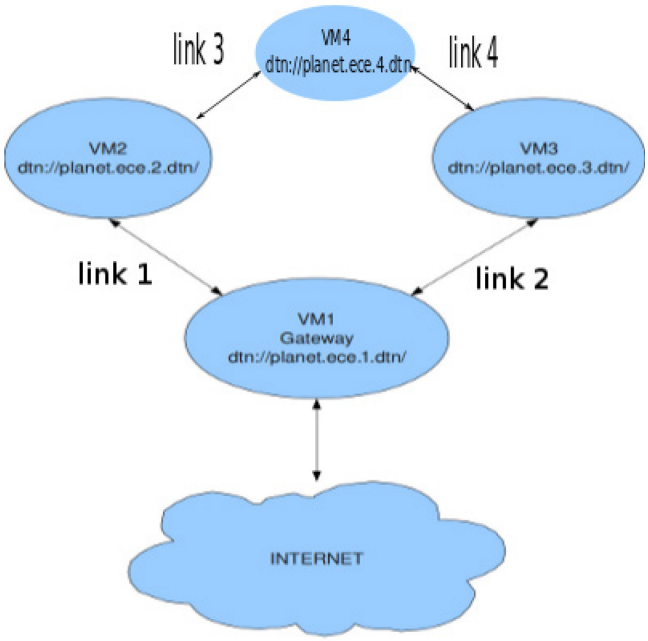

Figure 1: Overview of the DTN network set up at the University of Patras

2.3 Smart cameras and the surveillance task

The smart camera motes are based on the CITRIC platform [7]. The camera sensor is an Omnivision OV965 1.3 megapixel sensor. The mote is based on an ARM architecture Intel CPU with 64 MB of SDRAM used for temporary image storage and 16 MB of flash memory for permanent program storage. The motes run embedded Linux. Camera motes are connected to TelosB 802.15.4 adapters running TinyOS as to communicate between them and the base station.

The motes form a distributed wireless network based on the IEEE 802.15.4 protocol. The application running on the camera motes is a simple motion detection algorithm. Motion must be detected by at least two cameras in order for an event to occur. Cameras can communicate between them when events are recorded and when an event is confirmed by at least two of them, images from all cameras are transmitted to the storage unit via the IEEE 802.15.4 protocol. The surveillance application can easily be configured for sensitivity allowing for easy customization depending on location. The power consumed by the motes is minimal allowing for them to be powered by renewable sources such as solar power allowing for them to work in an autonomous way.

In order to create a realistic scenario for the network tests and to estimate amount of data needed to be transferred, smart camera motes were programmed to execute a regular motion detection process at a real environment in a university laboratory. After running the motion detection programs for a few days, it was found that typical size of data captured by the smart camera motes due to motion detection was at most of few tens of megabytes. As a result, it was chosen to use a package transmission of this order of magnitude for the conducted network tests as well as to assess possible storage needs.

2.4 DTN infrastructure and monitoring

The storage/DTN connectivity node is home to the saved images from the camera motes. A shared directory exists which all nodes can access and write to. A shell script periodically checks whether the link between the storage node and the outside world is up. When this is the case, it transmits all the saved images using the DTN protocol stack.

As mentioned earlier, the DTN connectivity/storage node runs the DTN stack. More specifically, it runs the DTN2 reference implementation version 2.7.0 of the Bundle protocol. Currently, the DTN2 reference implementation is considered to be the best-documented implementation of the Bundle protocol and one of the most widely used.

The storage node is part of a DTN network that is set up in the laboratory in order to study DTN issues and performance. The network is a multi-hop network in order to provide a realistic scenario since often DTN networks need multiple hops in order to reach nodes that can access a network of regular connectivity. In our case, the Bundle protocol runs over the TCP/IP stack and uses plain IP as the network protocol.

Since the DTN2 implementation does not contain any monitoring mechanism, our own monitoring mechanism was set up in order to assess the performance and stability of the network. The mechanism is based on shell scripts that parse and process log files produced by the DTN2 binaries. These logs are then passed to the Munin resource monitoring software that creates graphs and automatically visualizes the network status in an intuitive way. Details on the monitoring mechanism are provided in [8].

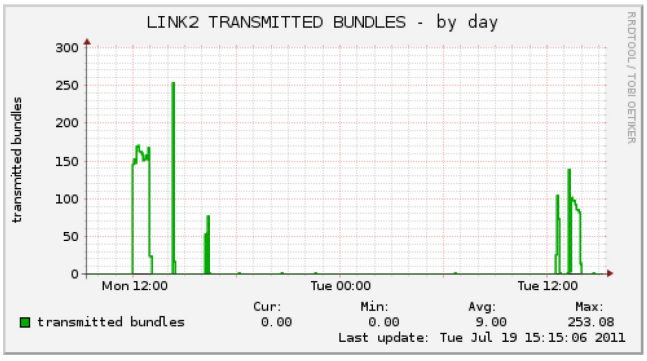

Figure 2: Example of the graphs provided by the developed monitoring mechanism. On the right of the graph it displays the number of Bundles transmitted with BSP enabled, first line, and without second line.

3. TESTING AND MEASUREMENTS

The aim of the conducted tests was to examine whether the proposed DTN network connection can be an alternative to regular connectivity. In order to do this, a scenario of intermittent connectivity was created. DTN links were switched between up and down status in order to simulate a true DTN scenario. Links changed status every few hours. A multi-hop DTN network structure was created in order to make the test more realistic. Tests were conducted for four different transmission methods. Methods chosen from the regular Internet were practically based on file transfer applications since Bundle transmission essentially performs this task. The four transmission methods that were tested were the following:

- DTN transmission with the Bundle protocol over TCP/IP
- DTN transmission with the Bundle protocol and the BSP security enabled over IP
- Clear text transmission over TCP/IP
- SCP transfer over TCP/IP

In the case of DTN transmission with BSP enabled, the BAB-HMAC cipher suite was used. SCP, or Secure Copy Protocol, is a method of securely transferring files by using the mechanisms provided by established SSH connections.

The parameters that we aimed to measure from the test were the throughput achieved in the transfer and the latency induced by each protocol. Moreover, by using the monitoring mechanism we aimed at testing the stability and reliability of these protocols in contrast to well-established protocols of the Internet as well as assess the level of security provided by the security mechanisms. Also, the monitoring mechanism allowed us to visualize and confirm test results. Results are average throughput of continuous 60 minute transmissions between virtual nodes residing on the same physical machine. Bundles or files used for the transfer were each of 60 MB size.

The summary of the test results that were performed appear in Table 1.

Table 1. Summary of Measurements

Protocol	Throughput	Latency
Bundle	14.00 MB/sec	15 ms
Bundle / BSP	6.23 MB/sec	15 ms
Cleartext IP	18.90 MB/sec	1 ms
SCP	12.00 MB/sec	1 ms

Results from the DTN measurements were obtained using the DTNperf tool that is included in the DTN2 implementation. This tool can accurately measure performance of the DTN network under all circumstances, including cases where a DTN BSP security policy is in place. Plain IP measurements were taken using the IPerf tool, a standard Internet performance measurement tool and the one DTNperf is based on. SCP measurements were performed in order to measure how a well-established secure method of transferring files can perform in comparison to the DTN transfers. There results were reported by the SCP client used.

All network experiments were held in the University campus LAN. As a result, latency is very small and is not a realistic value but it has a relative meaning to assess latency induced by the use of the protocol. Latency was measured using ICMP 'ping' packets [9] and the implementation of the DTN equivalent tool.

4. DISCUSSION OF RESULTS

4.1 Throughput

Throughput measurements are important because they can show whether the proposed DTN connectivity can provide a real network alternative. Since connectivity in DTN networks is interminant, when the links are available for a brief period, data should be transferred as fast and as efficiently as possible. The results show that although there is a slight decrease in throughput between transmission through the Bundle protocol and transmission through regular Internet protocols, this difference is not considerably significant. The difference most probably exists because of needed protocol processing and not the existence of extra headers or other information because these are relative small in the Bundle protocol.

Regarding reduction in throughput induced by BSP security mechanisms, this is quite significant and is measured at about 40% of the achieved throughput without security. This is similar, however, to the measured reduction induced by the SCP protocol in regards to the maximum performance of unencrypted communication. This means that BSP security does not induce more overhead to unsecured communication than what traditional security schemes induce to the regular internet protocols. This is important since unsecured communication is only examined for reference. In practice, transfer of data in a surveillance application always implement some sort of security mechanism.

4.2 Latency

Latency is of secondary importance to a DTN network compared to throughput because instead of frequent exchange of small amounts of data via a duplex communication link, our application more closely resembles exchange of larger amounts of data with fewer responses. However, latency does have some importance for operations such as key distribution or confirmation of reception.

From the results it is show that the Bundle protocol induced a round trip latency of about 14 milliseconds in addition to the minimal latency of the TCP/IP network. The latency is due to protocol processing and not the physical characteristics of the channel, which should be the same regardless of higher-level protocols. The amount of latency measured is relatively insignificant for the kind of applications intended for Delay Tolerant Networks.

4.3 Reliability and uptime

Reliability cannot be directly measured by a test however the DTN monitoring mechanism that has been developed allowed to reach some conclusions. All transfers that took place via the Bundle protocol provided reliable and accurate data transfer. Moreover, the system uptime was satisfactory with no monitored downtime of the Bundle Agents. Of particular importance were scenarios where links went offline during Bundle transfers. We observed that Bundles were retransmitted successfully, once the links became available again, without any loss of information.

5. CONCLUSIONS AND FUTURE WORK

From the tests and the overall experience with the system, we conclude that DTN connectivity and in particular the DTN2 implementation of the Bundle protocol provide a viable alternative to regular Internet protocols for applications such as smart camera surveillance in remote areas. The Bundle protocol provides an

acceptable performance, tested stability, and basic network security mechanisms. Therefore, we propose to extend smart camera surveillance use beyond real-time applications and fast connectivity.

In the near future, we intend to investigate the possibility to run the DTN stack autonomously on the smart camera motes and thus, eliminate the need for a proxy base station for connecting to the Internet. Moreover, a real surveillance environment of a remote area and a real physical disruptive link would help better confirm and validate the results obtained in the simulated environment.

6. REFERENCES

[1] Bramberger, M., Doblander, A., Maier, A., Rinner, B. and Schwabach, H. , "Distributed embedded smart cameras for surveillance applications," Computer , vol.39, no.2, pp. 68-75, Feb. 2006

[2] Durst, R., Feighery, P. and Scott, K., Why not use the Standard Internet Suite for the Interplanetary Internet?, MITRE White Paper, 2002.

[3] Scott, K. and Burleigh, S., Bundle Protocol Specification, IETF RFC 5050, Nov. 2007; www.rfc-editor.org/rfc/rfc5050.txt.

[4] Ramadas, M., Burleigh, S., Farrell, S., “Licklider Transmission Protocol – Specification,” IETF RFC 5326, Sep 2008; http://www.rfc-editor.org/rfc/rfc5326.txt

[5] Delay Tolerant Networking Research Group; http://www.dtnrg.org/.

[6] Ivancic, W., Wood, L., Holliday, P., Eddy, W.M., Stewart, D., Jackson, C. and Northam, J., , "Experience with Delay-Tolerant Networking from Orbit," *Advanced Satellite Mobile Systems, 2008. ASMS 2008. 4th* , vol., no., pp.173-178, 26-28 Aug. 2008

[7] Chen, P., Ahammad, P., Boyer, C., Shih-I Huang, Leon Lin, Lobaton, E., Meingast, M., Songhwai Oh, Wang, S., Posu Yan, Yang, A.Y., Chuohao Yeo, Lung-Chung Chang, Tygar, J.D. and Sastry, S.S., "CITRIC: A low-bandwidth wireless camera network platform", *Second ACM/IEEE International Conference on Distributed Smart Cameras, 2008*, vol., no., pp.1-10, 7-11 Sept.

[8] Papalambrou, A., Voyiatzis, A.G., Serpanos, D.N. and Soufrilas, P., "Monitoring of a DTN2 network," *Internet Communications (BCFIC Riga), 2011 Baltic Congress on Future*, vol., no., pp.116-119, 16-18 Feb. 2011
doi: 10.1109/BCFIC-RIGA.2011.5733226

[9] Postel, J., "Internet Control Message Protocol", IETF RFC 792, Sep 1981; http://www.ietf.org/rfc/rfc792.txt