2012 International Conference on Information and Computer Networks (ICICN 2012)
IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore

An Efficient Surveillance Data Management Scheme for Large-Scale Smart Camera Networks

Soomi Yang

Department of Information Engineering, The University of Suwon, Korea
smyang@suwon.ac.kr

Abstract. In large-scale smart camera networks, cooperation between devices is required for seamless tracking of targets. A large amount of multimedia data and derived metadata is generated and transferred between devices. In this paper, we design a large-scale surveillance system which is consisted of smart cameras. It complies with the standard specification to ensure interoperability between cameras and flexibility regarding the integration of new devices and services. Surveillance data contained in them if properly be structured and integrated, can induce useful context information. This paper builds a hierarchical surveillance data deploy structure and import related data from others to annotate data. The annotation process provides an impetus to the improvement of knowledge over time. We define management policies providing proactive surveillance data deploying and compare their performance for the large-scale surveillance.

Keywords: smart camera networks, large-scale surveillance system, metadata deployment, web service

1. Introduction

For the wide area surveillance, agents built in networked smart cameras explore the convergence of the data deploying and streaming technologies for multimedia data to collaborate through integration of metadata. We use the term metadata as defined in ONVIF(Open Network Video Interface Forum) specification[1] to include analytics, PTZ(Pan Tilt Zoom) status, events, and serial data. This paper describes a framework for the working of such a distributed surveillance data deploying and management system. Distributed agents receiving heterogeneous data from other sources have autonomy, collaborate with each other, and do ontology reasoning based on distributed knowledge bases.

In large-scale smart camera networks, cooperation between devices is required for seamless tracking of targets. In this paper we present a decentralized surveillance system complying with the ONVIF specification to ensure interoperability between cameras. Complying with standards provides flexibility regarding the integration of new devices and services, thus allowing to reduce costs and facilitate maintainability of the systems.

In the process of data analysis each agent may process the consolidated data for the distributed and autonomous reasoning, which is scalable and efficient[2]. It helps security persons by giving appropriate decision or prediction based on huge ontology data about situation it gathers. The representation of the generated metadata in a graphical user interface provides a comfortable overview of the surveillance area and brings easy integration of interaction of the security persons with devices.

The rest of the paper is organized as follows: Section 2 surveys related work of surveillance data management schemes. Section 3 describes our cooperative surveillance data management techniques. In Section 4, simulation and implementation result is presented and the performance is evaluated. Finally, Section 5 concludes.

2. Related Work

Surveillance systems based on various video and signal, have been developed and numerous studies are carried out on the multimedia data management techniques in distributed environments. Especially [3] dealt with multimedia data which is the most interested data format for the surveillance environment. However, previous works were mostly based on the ground that the distributed nodes in the network have the same characteristics, and the data transmitted is uniform and intermittent. Our distributed surveillance environment consisted of various data source devices, multimedia data and event data are generated continuously and analysis should be done in real time.

To ease merging of heterogeneous data, we need a framework based on a global standard. Effort for the standardization for physical security is done by ONVIF(Open Network Video Interface Forum)[1] and PSIA(Physical Security Interoperability Alliance)[4]. They define, recommend, and promote standards for IP-based security products. ONVIF has about 300 member companies and has greater influence than PSIA. Our system exchange data between all components in the surveillance network performs according to the ONVIF specification. It ensures the interoperability between devices and flexibility regarding the integration of new devices.

For a decentralized data networks management, [5] introduces distributed tracking system using ontology for cooperation. [6] suggests network buffer management which can be generally used , but is not specialized for surveillance networks. Many of wide area smart camera networks are closed system and do not provide surveillance information as a public web services which is suggested in the standard. We try to meet the standard and accomplish efficient surveillance data management.

3. Cooperative Surveillance Data Management

Our system named CUSST(Center for U-city Security and Surveillance Technology) is based on networked smart cameras with intelligent reasoning agents. Our framework architecture consists of a hierarchy of agents, which contains a number of non-leaf node administrative agents and leaf node agents with smart cameras. It consists of national agents at the top, some regional agents at the middle level, and many local agents at the second lowest level. At the lowest level, data source agents such as agents built in smart camera make leaf nodes.

The ONVIF has developed an open standard aiming to achieve the interoperability between networked video surveillance devices. The ONVIF specification defines a network layer of IP security devices described by web services. The definition of a surveillance service is provided by the WSDL(Web Services Description Language). WSDL document includes the definition of data types, messages, operations, and bindings. Data structure and exchange between web service requester and provider is based on the SOAP(Simple Object Access Protocol). Figure 1 shows XML schema example defined in AbsoluteMove class. Using apache-ant and apache-cxf we can produce java stub code as seen Figure 2 in part.

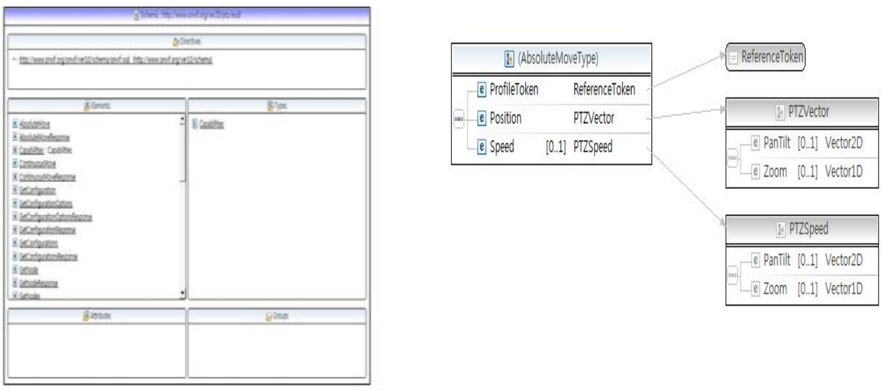

Fig. 1: An AbsoluteMove part of ONVIF XML schema

The processing of the surveillance data has moved from central servers to the decentralized smart camera agents. It may be fully distributed or clustered according to the administrative hierarchy. The data is analyzed within a camera agent, and the extracted information is forwarded to other camera agents.

```
@XmlAccessorType(XmlAccessType.FIELD)
@XmlType(name = "", propOrder = {
   "profileToken",
   "position",
   "speed"
})
@XmlRootElement(name = "AbsoluteMove")
public class AbsoluteMove {
@XmlElement(name = "ProfileToken", required = true)
   protected String profileToken;
   @XmlElement(name = "Position", required = true)
   protected PTZVector position;
   @XmlElement(name = "Speed")
   protected PTZSpeed speed;
```

```
public String getProfileToken() {
      return profileToken;
   }
public void setProfileToken(String value) {
      this.profileToken = value;
   }
public PTZVector getPosition() {
      return position;
   }
public void setPosition(PTZVector value) {
      this.position = value;
   }
public PTZSpeed getSpeed() {
      return speed;
```

Fig. 2: Stub code generated from WSDL description

Our surveillance data management framework assumes a proactive, rather than reactive, deploy of multimedia data and metadata. By proactive deploying, it means that the middle level agents cooperate with the master in exchanging necessary information on the data size, the request rate and so on enabling the master to fetch and broadcast the data before a lower level agents requests it. The system performances like hit rate, disk space, bandwidth gain of the agents and the leaf node source servers, bandwidth for the surveillance network, and latency experienced by the users are derived. We define *M* as the whole set of surveillance data, possibly segmented multimedia data and metadata, and assume that the data in *M* are ranked in the order of their suspiciousness or importance. From the well-known results that the probability of the i-th data is collected is Zipf distributed[2], we have the related probability function as Equation 1.

$$p(i) = \frac{c}{i^{\alpha}}, \forall i \in \{1, \cdots, M\} \tag{1}$$

where $c = \left(\sum_{i=1}^{M} i^{\alpha} \right)^{-1}$ and α is a normalization constant between 0 and 1. For the data replacement, our scheme selects a video block or metadata having the lowest weight. To maintain the freshness and effectiveness of the data, we should manage data adaptively. We use the term weight of data to describe its relative importance as compared to the other data according to FSR scheme as proposed in [7]. The higher the weight, the lower is the probability of the data being replaced. We also use a policy based on the size of the objects, in which the weight is proportional to the inverse of the size of the data for the network bandwidth usage efficiency. Therefore the weight *w* is computed as following, where *F* is the number of times the data is accessed, *S* is the size of the data and *R* is the time since the last access for the data. The three exponents *f* , *r* and *s* are weighting factor.

$$w = F^{f} S^{s} R^{r} = (d \cdot n_j \cdot \frac{c}{i^{\alpha}})^{f} \cdot (\sum_{i \in M} S_i)^{s} \cdot \mu_i^{r} \tag{2}$$

where *d* is a frequency factor, n_j is the total number of connected agents, and μ_i is the update interval. The value for *f* should be a positive number, meaning that more frequently accessed data is more likely to be found. The value of *s* should be a negative number for the efficient use of network bandwidth, such that more small data is more likely to be stored. The value of *r* should be a negative number, meaning that more recent data is more likely to be stored. If the recentness is more important than the frequency, the absolute value of the exponent *r* should be greater than that of the exponent *f*.

Our goal is to develop appropriate data transmission and caching scheme that minimize the mean transmission cost aggregated over all the surveillance data. It is assumed that a block of surveillance data *i* expires after an elapsed update interval *t* following an exponential distribution with average update interval μ_i. The corresponding probability density function and the survival function are,

$$f(t)=\frac{1}{\mu_i}e^{-\left(\frac{t}{\mu_i}\right)},S(t)=e^{-\frac{t}{\mu_i}} \tag{3}$$

If we let the probability of data miss according to a Poisson process with the same rate to keep the number of data miss in the system roughly constant, the probability of having data miss at each agent, L_i can be computed as following Equation (4),

$$L_i = 1-(1-e^{-\mu_i T})\cdot\frac{1}{\mu_i T} \tag{4}$$

$(1-e^{-\mu T})$ is the cdf(cumulative distribution function) of an exponential distribution. *T* is the maximum time it takes to detect the data miss. We can reduce the data miss probability L_i, with proactive data deploying according to the previously calculated weight *w*.

Then the required network bandwidth to transmit all the data updates, denoted by *B(t)*, is given by

$$B(t)=\sum_{i\in M}\frac{S(t)_i}{\mu_i}\cdot(1+L_i) \tag{5}$$

We use this metric as the performance parameter. Proactive data management to reduce this factor shows effiency as shown in performance evaluation section.

4. Performance Evaluation

4.1. Simulation

For the performance evaluation, the weight values and the required network bandwidth is calculated and compared.

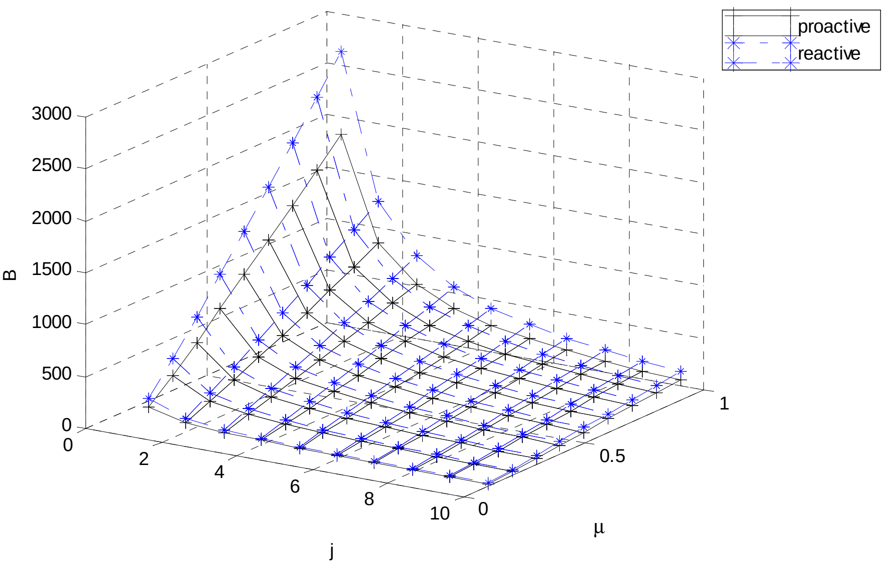

Fig. 3: Network bandwidth comparison

The data miss rate diversity with the data update interval and the weight threshold is shown in Fig. 3. In the figure, we show values in regard to the data update interval μ_i. For the adaptive deploying technique, we can raise the weight threshold value for the proactive caching. Our cooperative and proactive data deployment strategy shows more performance gain for the short update interval. When we increase the replacement threshold value, the required network bandwidth decreases.

4.2. Implementation

We implemented our cooperative data deploy framework for integrating surveillance data with an adaptive deploying technique into our decentralized surveillance system, CUSST.

Fig. 4: User interface implemented

Our systems were installed and tested under real campus conditions. The subject tracking through the communication between the independent smart cameras is possible as shown in Fig. 4. They inquire data for a combined inference through defined queries conforming ONVIF standard.

5. Conclusion

In this paper, we designed a large-scale surveillance system which complies with the ONVIF specification. The ONVIF specification defines a protocol for the exchange of information between surveillance devices. We use conformity to update and share data in a cooperative way on the ONVIF framework. The specification includes device discovery, video streaming, metadata and use of web services to efficiently provide interoperability between devices.

The system we present in this paper is composed of smart cameras whose captured video sequences are analyzed in its agent and exchange information with the neighbour agents. As user interface we implemented web interface and mobile interface provide comprehensive views of the monitored environment and offer the user an intuitive way to interact with surveillance devices.

Simulation studies and implementation are conducted to evaluate the effectiveness of our data management scheme. It shows the efficiency of our scheme resulted in better network bandwidth requirement. With our data distribution technique, agents can achieve very high hit rate locally, thus reducing significantly the bandwidth requirements of the network connection and the latency.

6. Acknowledgements

This work is supported by the GRRC program of Gyeonggi province. [GGA0801-45700, Center for U-city Security and Surveillance Technology, GRRC SUWON2012-B1].

7. References

[1] ONVIF (Open Network Video Interface Forum) http://www.onvif.org

[2] A. Schlicht and H. Stuckenschmidt, “Towards Distributed Ontology Reasoning for the Web,” WI-IAT08, 2008, pp. 536-539.

[3] T R Gopalakrishnan Nair, P Jayarekha, A Rank Based Replacement Policy for Multimedia Server Cache Using Zipf-Like Law, Journal of Computing, Volume 2, Issue 3, 2010

[4] PSIA Specification Package Q12009, http://www.psiaalliance.org

[5] J. Gomez-Romero, M. A. Patricio, J. Garcia, and J. M. Molina, “Communication in distributed tracking system: an ontology-based approach to improve cooperation,” Expert Systems (The Journal of Knowledge Engineering), Vol. 28, No. 4, 2011, pp. 288-305

[6] K. Chitra and Dr. G. Padmavathi, “FAVQCHOKE: To Allocate Fair Buffer to a Dynamically Varying Traffic in an IP Network,” International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.1, 2011, pp.73-81

[7] Paknikar, A., Kankanhalli, M., and Ramakrishnan, K., A Caching and Streaming Framework for Multimedia, ACM Multimedia, 2000