*2012 International Conference on Information and Computer Applications (ICICA 2012)*
***IPCSIT vol. 24 (2012) © (2012) IACSIT Press, Singapore***

# Cooperative Data Deployment Strategy in Wide Area Surveillance Networks

Soomi Yang and Pil Seong ParK +

Department of Computer Science, University of Suwon, South Korea

**Abstract.** In a decentralized wide area surveillance networks which cooperate with each other efficient data deployment strategy is needed for agile integrated reasoning. An overwhelming amount of multimedia data with event data and feature data is generated continuously by surveillance devices such as smart cameras or various sensors. 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 arriving from multiple data source devices. The annotation process provides an impetus to the improvement of knowledge over time. Proactive surveillance data deploying provides the main concepts and properties to model a hierarchical area data structure. We define management policies helping agent's reasoning process and compare their performance for the wide area surveillance.

**Keywords:** Data deployment strategy, Wide area surveillance system, Cooperative reasoning

## 1. Introduction

For the surveillance of the large area, agents built in networked RFID sensors, CCTVs and smart cameras explore the convergence of the data deploying and streaming technologies for multimedia data to collaborate through integration of other data such as device profile data, event data, biometric data and feature data. We use the term surveillance data to include audio, video, recognized feature data, ontology data and others. Most surveillance data transfers take place with the streaming data passing through one or more of the agents. Effective data deploy techniques will be critical for the successful deploy of streaming multimedia data over the surveillance network. This paper describes a framework for the working of such a distributed data deploying and management system. Distributed agents receiving heterogeneous data from various sources have autonomy, collaborate with each other, and do ontology reasoning based on distributed knowledge bases.

In the process of reasoning each agent may process the consolidated data for the distributed and autonomous reasoning, which is scalable and efficient[1], helps security persons by giving appropriate decision or prediction based on huge ontology data about situation it gathers.

The rest of the paper is organized as follows, Section 2 surveys related work of cooperative inference schemes. Section 3 describes the adaptive surveillance data management technique. In Section 4, implementation results are presented and the performance is evaluated. Finally, Section 5 concludes.

## 2. Related Work

Numerous studies have been carried out on the data management techniques in distributed environments. Especially [2] 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 standardized and intermittent. Our

+ Corresponding author.
*E-mail address*: smyang@suwon.ac.kr, pspark@suwon.ac.kr.

distributed surveillance environment consisted of various data source devices, multimedia data is generated continuously and analysis should be done in real time.

To ease merging of heterogeneous data, effort for the standardization for physical security is done by ONVIF(Open Network Video Interface Forum)[3] and PSIA(Physical Security Interoperability Alliance)[4]. They define, recommend, and promote standards for IP-based security products. Our implemented system tried to meet the requirements of industry by providing functions recommended by standard organizations.

For a decentralized surveillance 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 surveillance 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 framework architecture consists of a hierarchy of agents, which contains a number of non-leaf node administrative agents and leaf node agents with sensors. 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 servers can communicate each other freely within access control permission to perform their own intelligent distributed context inference based on their own ontology knowledge base integrated with imported ontology data. Agents in each server is built and communicate each other following the ONVIF standard as seen in Fig. 1.

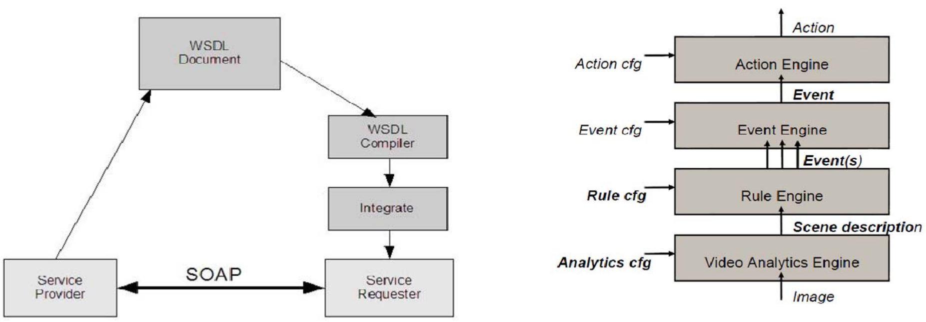


Fig.1. Standard web service configuration in ONVIF [3]

Deploying data in surveillance network has usually a hierarchical architecture on top of the hierarchical administration organization. These data, often referred to as institutional, regional, and national data depending on the hierarchy of the administrative agents operating them, is integrated with each other so as to infer and deliver efficiently the requested result to the users. For distributed data, even small agents, with the help of higher level agents, can achieve very high hit rate locally, thus reducing significantly the bandwidth requirements of the network connection and the latency perceived by the users.

Our system framework assumes a proactive, rather than reactive, deploying of data. 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. To achieve this goal, the surveillance network is modeled as a multi-layered distribution network as in the next section. 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. Single server with CCTV is constructed as seen in Fig. 2.

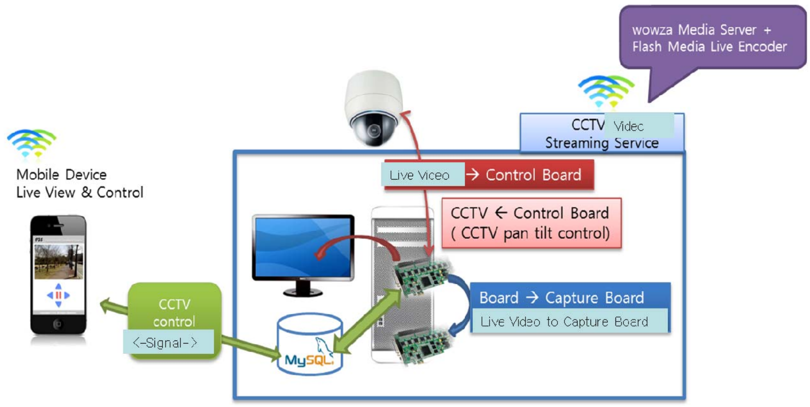


Fig. 2. Single site constitution with CCTV

For the performance analysis, we specify some features of the forwarding data in multi-layered network. We define $D=\{1,2,\ldots,|D|\}$ as the whole set of data, and assume that the data in $D$ are ranked in the order of their suspiciousness or importance. From the well-known results that the probability of the $i$-th data is Zipf distributed, we have the related probability function [2].

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 as proposed in [7]. The higher the weight, the lower is the probability of the clip 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. Every agent operates the same set of data for some designated suspect, the expression for $\delta_k$ being the same and independent to the other connected agent $k$.

$$\begin{aligned} W &= F^f S^s R^r \\ &= \lambda_{ki}^f \delta_k^s \mu_i^r \qquad (1) \\ &= \left(\beta n_k \bullet \frac{\sigma}{i^a}\right)^f \bullet \left(\sum_{i \in D_F} S_i\right)^s \bullet \mu_i^r \end{aligned}$$

where $\mu_i$ 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 can be 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 $f$.

With the same preference distributions and the same set of data, all the subscribing agents have the same hit rate as a distributed surveillance environment and multimedia data and feature data are produced continuously. 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 server, $P$ can be computed as following Equation (2),

$$P = 1 - \left(1 - e^{-\mu T}\right) \bullet \frac{1}{\mu T} \qquad (2)$$

$\left(1-e^{-\mu T}\right)$ 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 $P$, with proactive data deploying according to the previously calculated $w$.

## 4. Performance Evaluation

For the performance evaluation, the data miss rate is calculated according to the following Equation (3).

$$Q=\left(f\left(p\right)-f\left(w\right)\right)/f\left(p\right) \tag{3}$$

where *f(P)* is the amount of the data miss according to the Equation (5) and *f(w)* is the amount of the prefetched data based on the Equation (2). The data miss rate diversity with the data update interval and the weight threshold is shown in Fig. 3. Because other factors such as data rank, size, etc., there are many surplus values plotted in the graph. In the figure, we show values in regard to the data update interval $\mu_i$. Our cooperative and proactive data deployment strategy shows more performance gain for the short update interval. For the adaptive deploying technique, we can raise the weight threshold value for the proactive caching. When we increase the threshold value, the data miss rate $Q$ decreases resulting in better data integration for cooperative reasoning.

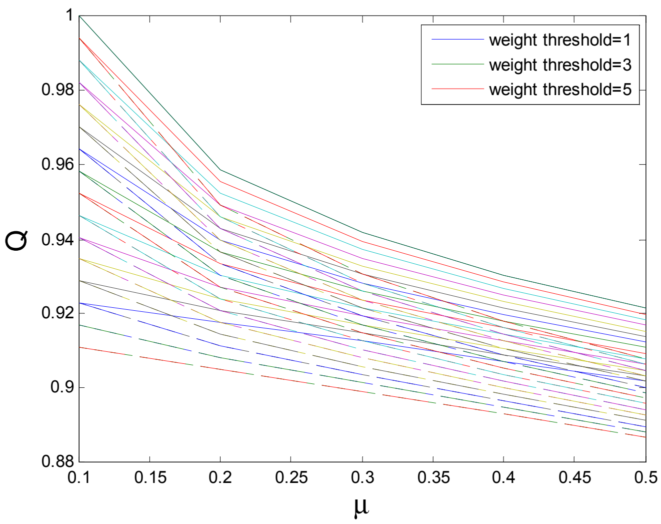


Fig. 3. The data miss rate diversity with the data update interval and the weight threshold

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

The subject tracking through the communication between the independent agent is possible as shown in Fig. 4. They inquire feature data for a combined inference through defined queries conforming standard. In Fig. 4, implemented web interface and mobile interace is shown.

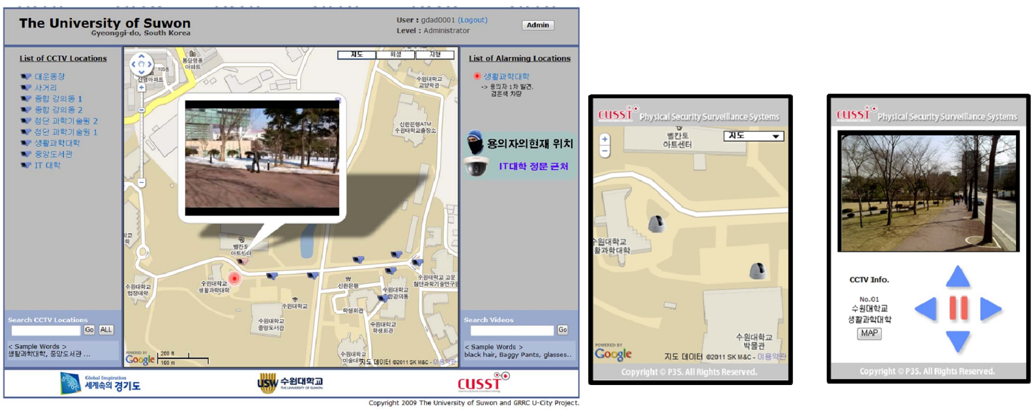


Fig. 4. Subject tracking between several smart cameras

## 5. Conclusion

In this paper, we propose a flexible surveillance data deploying scheme which is adaptive to the actual device demands and that of its neighbors. Our scheme uses conformity to update and share data in a cooperative way on the standard framework. It helps cooperative inference performed in each agents. Simulation studies are conducted to evaluate the effectiveness of our flexible surveillance data deploying scheme. Implementation is also going on into our wide area decentralized surveillance network environment. Based on mathematical derivations, the proactive deployment of surveillance data maximizes the reasoning engine's potential for making decisions from operating the hierarchical structure distribution. Computational experiments investigate how the optimal deployment scheme and service policy responds to system parameter changes. It shows the efficiency of surveillance data deploying resulted in better integrated context inference.

## 6. Acknowledgments

This work is supported by the GRRC program of Gyeonggi province. [GGA0801-45700, Center for U-city Security and Surveillance Technology, GRRC SUWON2011-B1]

## 7. References

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

[2] 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

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

[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