Sensors and Materials, Vol. 29, No. 7 (2017) 997–1003
MYU Tokyo

S & M 1391

Efficient Cooperative Inference Architecture for Reasoning Agents in Context-Aware Surveillance Networks

Soo-Mi Yang*

Department of Information Engineering, The University of Suwon
Wauangil 17, Hwasungsi, Korea

(Received May 2, 2016; accepted May 10, 2017)

Keywords: surveillance, information centric network, weighted ontology, cooperative inference, context-aware reasoning agents

In this paper, we investigate the model of multicamera, multisensor surveillance networks. To accomplish context awareness in wide area surveillance, several reasoning agents are distributed to analyze and process various events. Context ontology provides a more manageable and scalable representation of surveillance data for reasoning. For cooperative reasoning, agents exchange context knowledge to draw an integrated higher inference. Integrating heterogeneous ontologies is important for inference agents utilizing multiple ontologies. In this paper, architecture based on information-centric networking is proposed for a more efficient surveillance data delivery. Increasing surveillance data across areas generates concerns regarding the cost of transferring large amounts of event-related data sets. In an information-centric network, content is delivered over content stores and caching desired data from them can save bandwidth. In the proposed scheme, delivering semantically similar content within threshold values given in interest packets further reduces traffic. Estimation of similarity incorporated with weighted ontology, which considers trust level, importance and cost, provides efficient use of cache capacity. An experimental validation of the proposed method analyzes the cost of data transmission. Simulations show that the given information-centric architecture enables high reliability and performance with low transmission costs.

1. Introduction

For a context-aware intelligent surveillance system, each observation device is equipped with a customized reasoning agent. Agents first collect sensed data, extract features from raw data, then perform context reasoning to understand the present situation and derive related decisions. For context reasoning, agents use ontologies and knowledge bases built from ontologies as data. An ontology is a formal naming and definition of the types, properties, and conceptual relationships of the entities in a particular domain.[1] An ontology together with a set of individual instances of classes constitutes a knowledge base. The context ontologies used in this paper are hierarchically structured specifications of surveillance concepts, properties and relationships. To achieve a higher level inference, each agent requires data from peers. For cooperation between agents, a more efficient and scalable ontology data management framework is required.

*Corresponding author: e-mail: smyang@suwon.ac.kr
http://dx.doi.org/10.18494/SAM.2017.1601

ISSN 0914-4935

Information-centric networking (ICN)[2,3] is an approach to support named data by enabling in-network caching and replication. It reduces bandwidth provision costs by providing improved efficiency, scalability, and robustness.

Several intelligent systems based on ontology have been developed for querying and reasoning semantic knowledge as seen in Refs. 4 and 5. However, they do not utilize ICN for knowledge integration. A cooperative cache scheme for peers is described in Refs. 6 and 7; it combines peer-to-peer (P2P) communication technology with a conventional mobile system. However, the authors did not apply their technique to a cooperative surveillance system. In this paper, we propose an efficient context inference system utilizing ICN for urban security.

In the proposed system, each agent tries to be context-aware through integration, analysis, and inference of data. As an ontology integration scheme, data weighting and similarity measure updated cached data in an efficient and cooperative way. Experiments were conducted to evaluate the effectiveness of the suggested cache management scheme, and its implementation will be developed in future work.

The rest of the paper is organized as follows. In Sect. 2, the architecture of the proposed system is presented. In Sect. 3, the model for cooperative reasoning in context-aware network computing is explained. Experiments and implementation are demonstrated in Sect. 4, and in Sect. 5, we conclude this paper.

2. Architecture of the Cooperative Inference System

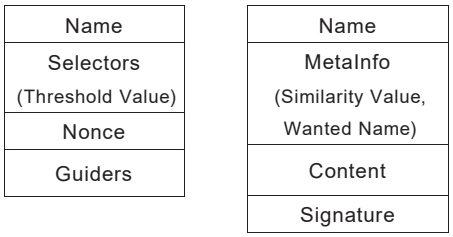
A surveillance system for urban security is a complex application that handles distributed multimedia. Surveillance systems deploy a network of sensors to monitor a wide area. For global event monitoring and situation awareness, it is crucial to detect and model correlations among events observed across sensors. Affluent data from which useful context can be inferred are acquired through diverse sensors. These data can include real-time sensed data, stored multimedia data, acquired event data, and extracted biometric feature data.

Because each sensor only preprocesses a certain part of the situation, additional processing is required to obtain the overall situation. By combining and integrating data from diverse sensors, context information that was not previously available in a single sensor can be achieved.

When developing a model capable of such integration as proposed in Sect. 3, utilization of ontologies is preferable owing to their high and formal expressiveness as well as the possibility of applying ontological reasoning techniques. Specifically, hierarchically organized feature space for context is employed. Thus, modelling correlations between events detected from multiple sensors throughout a wide area can facilitate global activity analysis.

In the proposed surveillance system architecture based on ICN, agents exchange interest and data packets for data acquisition. There are numerous approaches aimed at defining the reference ICN framework. Because named data networking (NDN) is the prevalent design of proposed ICN architectures, we defined the interest and data packet format as shown in Fig. 1, similarly to the format of NDN projects.[8] Here, the threshold value, v_t ($0 < v_t \leq 1$), is included in selectors. Moreover, the similarity value, v_s ($0 < v_s \leq 1$), and WantedName, which was originally "Wanted Name" in the interest packet, were included in MetaInfo.

Figure 2 shows the interest and data packet forwarding structure.[9] A pending interest table (PIT) stores all the interests not satisfied. The forwarding information base (FIB) maps name in Interest



(a) (b)

Fig. 1. Format of interest and data packets. (a) Interest packet. (b) Data packet.

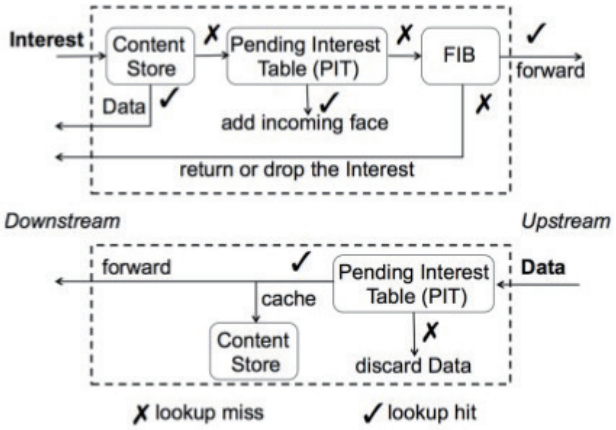


Fig. 2. ICN packet forwarding structure.

packet to physical network interfaces. Content store (CS) caches content in data packets to satisfy future interests. For the efficient use of limited cache space, a replacement strategy based on the weight measurement is required.

3. Model for Context-Aware Network Computing

A novel analysis framework is formulated to discover and quantify causal relationships among regional sensors. Global circumstances are inferred by correlating regional events from multiple sensors. Correlated context data across multiple sensors should be modelled collectively. By utilizing evidence collected from different sensors, global context inference modelling is more robust with respect to noise and ambiguities than modelling within individual sensors.

To model forwarding surveillance data to other agents, we assume that the data in the set of surveillance ontology are ranked in order of their popularity. The probability of the i-th data is Zipf-like distributed, with its probability function as shown in Eq. (1).[10]

$$f(i) = \frac{\sigma}{i^{\alpha}},\ i = 1, 2, \ldots, n \tag{1}$$

Here, $\sigma = 1/\sum_{i=1}^{n}(1/i^{\alpha})$, and α is the normalization factor depending on the application. The generalized harmonic number of order n of α is given by $H_{n,\alpha} = \sum_n i^{-\alpha}$ and $\sum_{i=1}^{n} f(i) = 1$, and σ can be roughly calculated as[11]

$$\sum_{i=1}^{n} f(i) = 1 = \sigma \cdot H_{n,\alpha} \approx \sigma \cdot \frac{n^{1-\alpha}}{1-\alpha},\ (\alpha \neq 1), \tag{2}$$

$$\sigma = \frac{1-\alpha}{n^{1-\alpha}}. \tag{3}$$

Let n_k be the total number of connected agents and λ_k, the data request rate. Because λ_k is proportional to n_k, the request rate of agent k for the data i, denoted by λ_{ki}, can be written as

$$\begin{aligned} \lambda_{ki} &= \lambda_k \cdot f(i) = c \cdot n_k \cdot \frac{\sigma}{i^\alpha},\ c > 0 \\ &= c \cdot \frac{n_k}{i^\alpha} \cdot \frac{1-\alpha}{n^{1-\alpha}}. \end{aligned} \tag{4}$$

Surveillance ontology data are produced continuously. To maintain the freshness and effectiveness of the data, cached data in CS should be continuously adapted. The weight of cached data is measured in a similar way as in Ref. 12 to describe its relative importance compared with other data. The higher the weight, the lower is the probability of the data being replaced. The weight ω_{ki} for data i in agent k is computed as in Eq. (5), where F is the number of times the data are accessed, R is the time since the last access, G is the SimilarityValue in data packet ($\forall i$, ($Sim(C_i,WantedName)$) $\geq$ *ThresholdValue*), and O is the ontology weight. The term $Sim(C_i,C_j)$, a similarity value between concept C_i and C_j, is a property derived from a set of distant concepts shared by both.[13] The four exponents, f, r, g, and o, are weighting factors. Relative importance is controlled by adjusting the exponent.

$$\begin{aligned} \omega_{ki} &= F^t R^r G^g O^o \\ &= \left(c \cdot \frac{n_k}{i^\alpha} \cdot \frac{1-\alpha}{n^{1-\alpha}} \right)^f \mu_i^r \cdot SimilarityValue(C_i)^g \cdot w(C_i)^o \end{aligned} \tag{5}$$

In Eq. (5), μ_i is the update interval and $w(\cdot)$ is the ontology weight, meaning trust level and/or importance, with $\forall i$, $0 < w(C_i) \leq 1$.

To build an efficient architectural model for CS management, the distribution of the data based on the statistical population is analyzed. In exponential distribution with the rate parameter μ, the probability of missing data in agent k can be obtained as $P_k = 1 - (1 - e^{-\mu t})/\mu t$. Let h be the number of hops that requested data traverse from source agent or CS to requestor. The cache replacement rate Q is given by Eq. (6).

$$Q = 1 - (1 - P_k)^h = 1 - \left(\frac{1 - e^{-\mu t}}{\mu t} \right)^h \tag{6}$$

On the basis of Ref. 14, the probability of a request for object D_j resulting in a hit can be approximated by $h_j = 1 - e^{-\lambda_i T}$, where T is the given constant for each cache. Let D_k be the set of surveillance ontology data required by agent k and S_i be the size of the i-th data. Then, agent k needs disk space δ_k as shown in Eq. (7).

$$\begin{aligned} \delta_k &\leq \sum_{j \in D_k} S_j \\ &= \sum_{j \in D_k} f(j) \left(1 - e^{-\lambda_j T} \right) \cdot S_j \end{aligned} \tag{7}$$

The latency, L_k, can be derived as shown in Eq. (8). Each agent and router generates control and data traffic. Following data caching, the update operation, the replacement operation, and the maintenance operation are generated targeting PIT and FIB.

$$L_k = \sum_{i=1}^{h} \frac{(SizeRequest + SizeReply) \cdot (control + data)}{Bandwidth} \frac{1}{1-p} \cdot (1 - P_k) \tag{8}$$

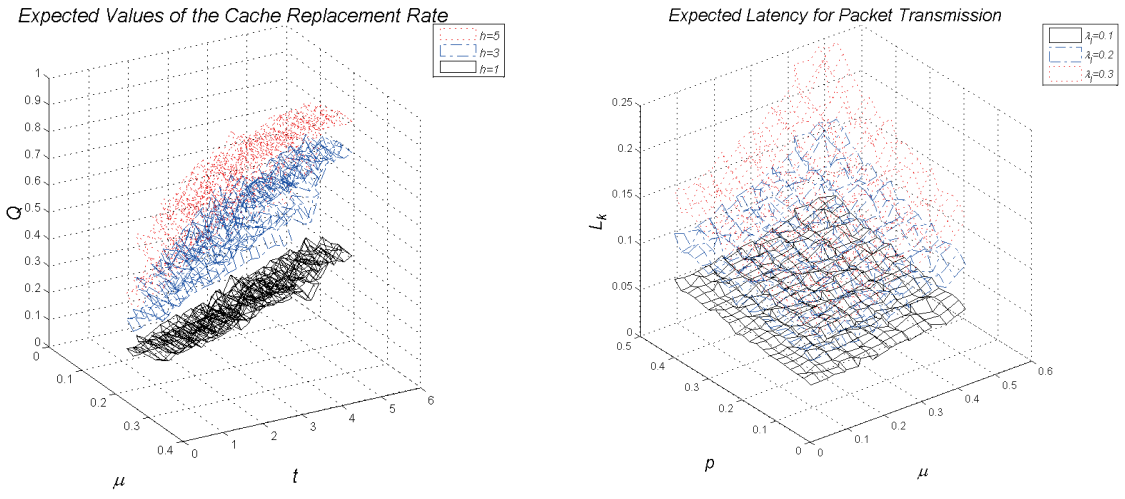
Here, p means the probability of packet loss during network transmission. The amount of data can be calculated using Eq. (7).

4. Experiments and Implementation

To evaluate the performance of the proposed model, experiments to measure the system performance metrics were carried out. From Eqs. (1)–(8), the cache weight, replacement rate, and latency for packet transmission were estimated.

Figure 3 (a) shows the cache replacement rate for missing data. For each given data missing rate μ, the effect on the cache replacement by the number of hops was inspected. Reducing the number of hops utilizing ICN improved the system performance. Figure 3(b) shows the expected latency for packet transmission according to μ and p with their increase in latency in general. More traffic with higher data request rates, λ_j, increased latency. For the adaptive deployment scheme, decreasing λ_j by raising the threshold value can proactively cache data. Moreover, when the threshold value was increased, the cache replacement rate, Q also decreased.

Our project belongs to the Center for U-City Security and Surveillance Technology (CUSST).[15] To build the proposed cooperative inference architecture into CUSST, a surveillance system with context ontologies will be further developed. Figure 4 shows part of its user interface. In a prototype system, identified events and feature data for context-aware computing are being



(a) (b)

Fig. 3. (Color online) Experiment results for cache management scheme. (a) Expected values of the cache replacement rate. (b) Expected latency for packet transmission.

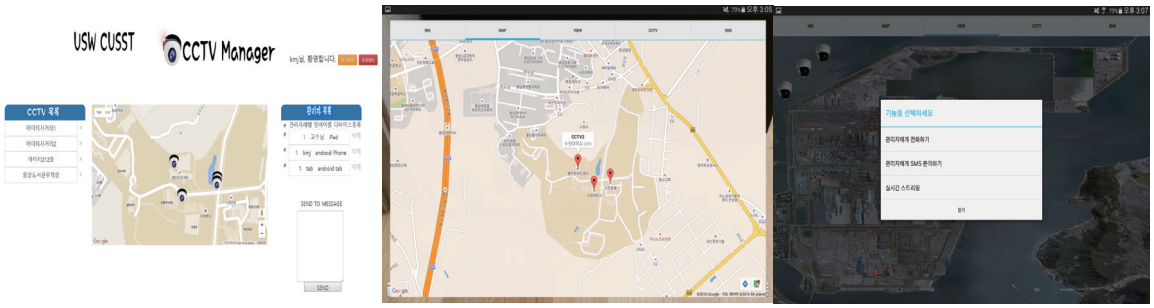


Fig. 4. (Color online) Screenshots of CUSST administration interfaces.

structured for similarity measurement into knowledge bases. Sensors are registered through menus for administrators. Reasoning agents process data, which are acquired from sensors, and CUSST displays various forms of inference results.

5. Conclusions

In this study, we investigated an efficient and scalable inference infrastructure for multicamera, multisensor surveillance networks. The surveillance data in an ontology knowledge base can include real-time sensed data, stored multimedia data, acquired event data, and analyzed biometric feature data. For better inferencing ability covering a broader area, ontologies in the area should be merged and aligned according to their semantic similarity. Adapted smaller ontologies help strengthen reasoning ability and the efficiency of network bandwidth use. Furthermore, providing semantically similar data to reasoning agents enhances inference efficiency.

The forwarding strategy in ICN consults the weight of cached data. Data weighing and information similarity measuring, which update and share data in a cooperative way, enhance the performance of data management. Data are cached in CS based on the analysis of the content distribution and the designated weighting scheme to reduce packet transmission frequency and latency.

Acknowledgments

This work was supported by the GRRC program of Gyeonggi Province (GRRCSUWON2016-B1, Center for U-City Security and Surveillance Technology).

References

1 N. Guarino: Proc. Formal Ontology in Information Systems (IAOA, Trento, 1998) p. 81.
2 IRTF: Homepage of IRTF Information-Centric Networking Research Group (ICNRG), https://irtf.org/icnrg (accessed July 2016).
3 G. Xylomenos, C. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. Katsaros, and G. C. Polyzos: IEEE Commun. Surv. Tutorials **16** (2014) 1024.
4 N. D. Rodríguez, M. P. Cuéllar, J. Lilius, and M. D. Calvo-Flores: ACM Comput. Surv. **46** (2014) 43.
5 A. Schlicht and H. Stuckenschmidt: Proc. IEEE/WIC/ACM Int. Conf. Web Intelligence and Intelligent Agent Technology (IEEE, New York, 2008) p. 536.

6 L. Yin and G. Cao: IEEE Trans. Mobile Comput. **5** (2006) 77.
7 J. Zhao, P. Zhang, G. Cao, and C. R. Das: IEEE Trans. Parallel Distrib. Syst. **21** (2010) 229.
8 Named Data Networking (NDN) Project, http://named-data.net/ (accessed July 2016).
9 L. Zhang, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang: ACM SIGCOMM Comput. Commun. Rev. **44** (2014) 66.
10 L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker: Proc. 18th Annu. Joint Conf. IEEE Computer and Communications Societies (IEEE, New York, 1999) pp. 126–134.
11 A. Sofo: Appl. Math. Comput. **207** (2009) 365.
12 A. Paknikar, M. Kankanhalli, and K. Ramakrishnan: Proc. 8th ACM Int. Conf. Multimedia (ACM, New York, 2000) p. 13.
13 D. Rajagopal, E. Cambria, D. Olsher, and K. Kwok: Proc. 22nd Int. Conf. World Wide Web Companion (ACM, New York, 2013) p. 565.
14 H. Che, Z. Wang, and Y. Tung: INFOCOM 2001, 20th Annu. Joint Conf. IEEE Computer and Communications Societies (IEEE, New York, 2001) p. 1416.
15 CUSST (Center for U-City Security and Surveillance Technology), http://grrc.suwon.ac.kr (accessed July 2016).

About the Author

Soo-Mi Yang received her B.S., M.S., and Ph.D. degrees in computer engineering from Seoul National University of Seoul, Korea, in 1985, 1987, and 1997, respectively. From 1988 to 2000, she was a researcher at the Korea Telecom Research Center where she worked on telecommunication network, internet and information security. From 2000 to 2001, she was a visiting scholar at UCLA, USA. From 2002 to 2004, she was a faculty member of the Suwon Science College, Korea. She is currently an associate professor with the Department of Information Engineering, The University of Suwon, Korea. Her research interests include access control, network security, and secure system software.