Multimedia Traffic Security Architecture for the Internet of Things

Liang Zhou, Nanjng University of Posts and Telecommunications
Han-Chieh Chao, National Ilan University

Abstract

An important challenge for supporting multimedia applications in the Internet of Things is the security heterogeneity of wired and wireless sensor and actuator networks. In this work, we design a new and efficient media-aware security framework for facilitating various multimedia applications in the Internet of Things. First, we present a novel multimedia traffic classification and analysis method for handling the heterogeneity of diverse applications. Then a media-aware traffic security architecture is proposed based on the given traffic classification to enable various multimedia services being available anywhere and anytime. Furthermore, we provide a design rule and strategy to achieve a good trade-off between a system's flexibility and efficiency. To the best of our knowledge, this study is the first to provide general media-aware security architecture by jointly considering the characteristics of multimedia traffic, security service, and the Internet of Things.

The Internet of Things (IoT) is a novel network architecture that is rapidly gaining attention in the scenario of next-generation wireless telecommunications. The basic idea of IoT is pervasively providing us with a variety of things or objects, such as radio frequency identification (RFID) tags, sensors, actuators, and mobile phones, which are able to interact and cooperate with each other to realize the tasks of communication, computation, and service [1]. Such a network poses a bright foreground for large-data multimedia applications as demand for emerging applications like video on demand (VoD), IPTV, and voice over IP (VoIP) has grown tremendously [2]. Figure 1 provides a classic example of multimedia service architecture in the context of IoT.

Nowadays, security is of critical importance for various multimedia applications in IoT [3]. Since the IoT is built to broadly execute unverified user-implemented applications from different users, both applications and users can be sources of security threats to the IoT [4, 5]. For example, the vulnerabilities of applications and sensors can be exploited by hackers, and malicious users can access the IoT to launch vicious service attacks. Moreover, a legitimate user may tamper with shared multimedia data or excessively exhaust network resources to interrupt services available to other legitimate users. On the other hand, however, the existing IoT has not employed a specific security mechanism to deal with the threats mentioned above [5]. Thus, it is very important and necessary to deploy a security strategy to protect security-critical multimedia applications streaming over the IoT.

As we know, traffic management plays a key role in achieving high multimedia quality of service (QoS) in a network [1]. Unfortunately, conventional multimedia traffic management algorithms, developed mainly to guarantee delay and distortion constraints while usually neglecting security requirements, are not appropriate for security-aware multimedia applications. In this article, we propose a security-critical multimedia service architecture in the IoT context, which jointly considers traffic analysis, security requirements, and traffic scheduling for multimedia applications. To illustrate the effectiveness, the proposed media-aware traffic security architecture (MTSA) is applied to obtain satisfying traffic management based on the given media-aware traffic classification and analysis. MTSA is one of the first security-aware traffic management strategies for multimedia applications running over the IoT. The fundamental contributions of this article include the following aspects:

- Traffic classification and analysis for various multimedia applications streaming over IoT
- Developing a novel architecture for media-aware traffic security
- Designing and evaluating the proposed security-critical traffic management scheme

The rest of this article is organized as follows. We present the multimedia traffic classification and analysis in the context of the IoT. We provide the media-aware traffic security architecture and specify the interaction and cooperation between the different parts. Moreover, the corresponding design rule and strategy are proposed. Finally, we conclude this article.

Multimedia Traffic Classification and Analysis

The characteristics of the IoT make it possible to develop a huge amount of multimedia traffic. Usually, an IoT is realized by equipping multiple sensors with high intelligence of communication, computation, and service capabilities. Specifically, we can divide the multimedia traffic running over IoT into three categories: communication, computation, and service. In this section, we analyze the above three kinds of multimedia traffic. Figure 2 illustrates multimedia traffic classification and analysis in the context of an IoT.

0890-8044/11/$25.00 © 2011 IEEE

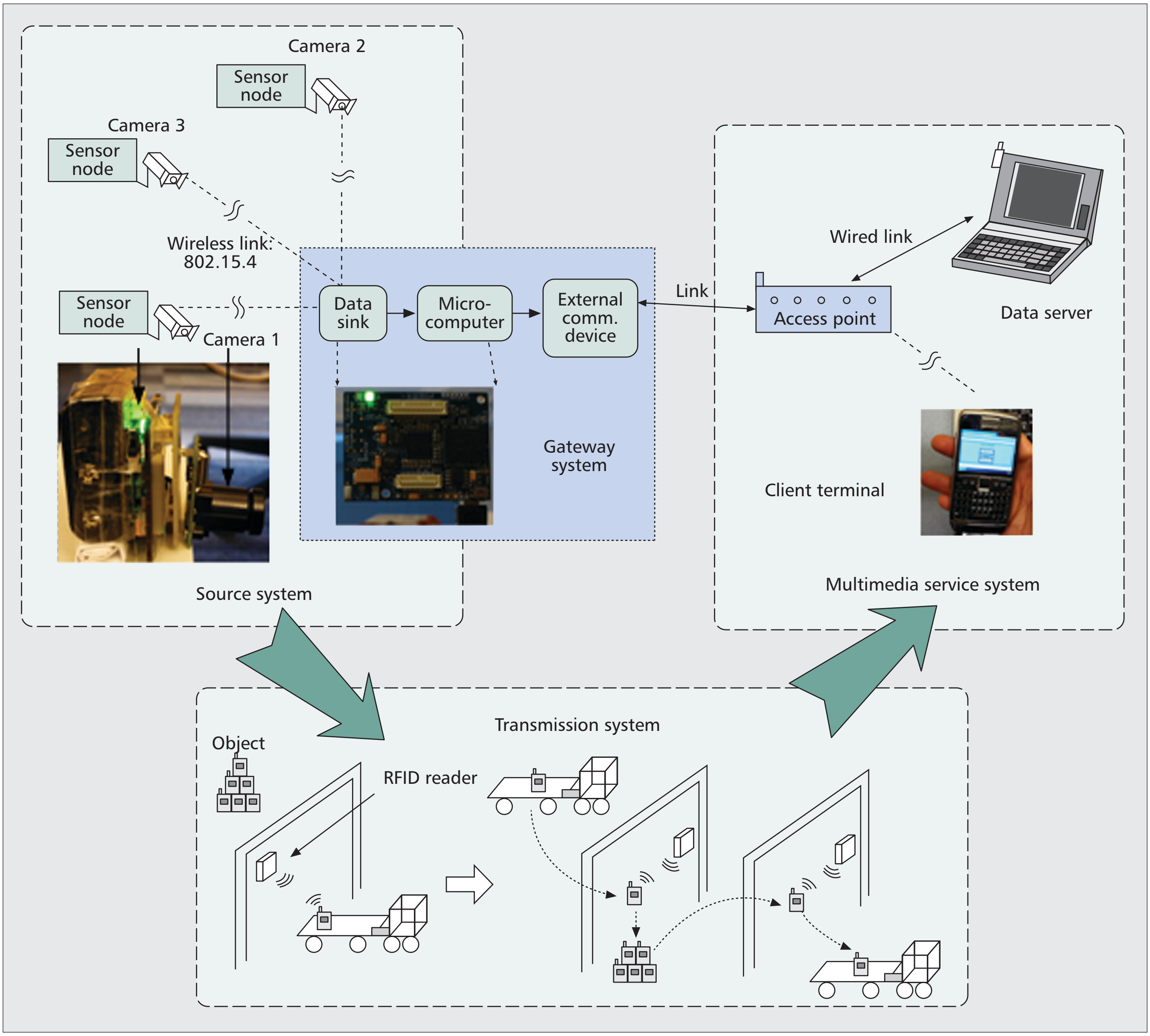

Figure 1. *An example of multimedia service architecture in the context of IoT [6].*

Communication Traffic

"Anytime, anywhere, anymedia" has been the communications goal for the IoT. In this context, the core component is an RFID system that consists of several readers and RFID tags. Each tag is characterized by a unique identifier and applied to different objects. Readers trigger tag transmission by generating a message, which represents a query for the possible presence of tags in the circumference of the reader [6]. For a practical IoT, an RFID tag is a small microchip attached to an antenna, and the antenna is used for both receiving the reader's message and transmitting the tag ID to the reader.

Actually, sensor networks are the major components of an IoT, and they can cooperate with RFID systems to complete the communication function. As we know, sensor networks are composed of a number of sensing nodes communicating in a multihop fashion. Usually, nodes report the results of their sensing to sink nodes. As to the communication traffic over the IoT, IEEE 802.15.4 does not include specifications on the higher layers of the protocol stack, which is necessary for the seamless integration of sensor nodes into the Internet [1]. Therefore, how to design appropriate communication traffic is an interesting and changeling task:

- The maximum physical layer packet in the framework of IEEE 802.15.4 is 127 bytes, while the maximum frame size at the medium access control (MAC) layer is 102 bytes. Moreover, due to the security algorithm employed at the link layer, which results in overhead, the frame size may further decrease [2].
- Different from traditional IP networks, in many scenarios sensor nodes are set in sleep mode to save energy and cannot work during communication periods.

In general, integrating sensing technologies into passive RFID systems would enable various multimedia traffic types available in the IoT context. Recently, several works have been conducted in this area. For example, a project on wireless identification and sensing platforms is being carried out at Intel Labs, powered and read by standard RFID readers, harvesting the power from the reader's querying message [6]. Briefly speaking, the objectives of designing appropriate multimedia traffic are energy efficiency, scalability, reliability, and robustness.

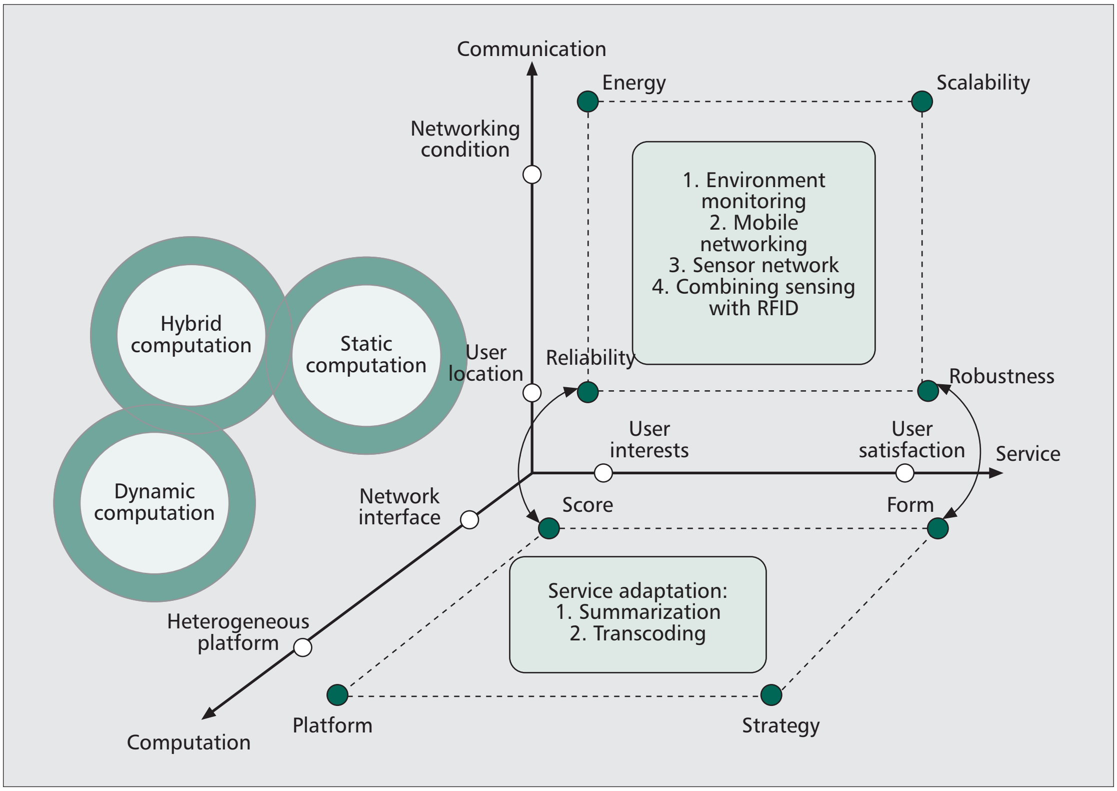

Figure 2. *Multimedia traffic classification and analysis in the IoT context.*

Computation Traffic

Usually, computation traffic over an IoT can be processed by mobile agents or sink nodes autonomously. The sequence in which a mobile agent visits the selected source nodes can have a significant impact on computation traffic [1]. Note that finding an optimal source-visiting solution is a typical non-deterministic polynomial-time-complete problem [3]. Computation traffic can be categorized as follows:

- *Static computation:* The computation state of the mobile agent is determined by the source node before it is dispatched.
- *Dynamic computation*: The agent autonomously determines the source nodes, and decides the dynamic route or resource allocation according to the current network conditions.
- *Hybrid computation*: The set of source nodes is decided by the sink nodes, while the source-visiting sequences are processed by the mobile agents.

Static Computation — It makes use of current global network conditions and finds an efficient path before the mobile agents are sent. In [1], the authors summarize two approaches, Local Closest First (LCF) and Global Closest First (GCF). Specifically, both approaches start at the sensor node closest to the dispatcher. When source nodes intend to form multiple clusters with similar distance to the sink, GCF causes zigzag routing due to the itinerary fluctuations among those clusters.

Dynamic Computation — Because the global information collected at the sink node may become outdated due to variations over the IoT, dynamic computation can enable the mobile agents or sink nodes to decide the next hop at each step of the routing establishing process. In addition, in the process of deciding a dynamic route, it is necessary to take into account the trade-offs between the cost of migration and the benefit of migration accuracy. The dynamic computation approach seeks the sensor node that satisfies both the largest available remaining energy and the least energy consumption for the agent's migration.

Hybrid Computation — In hybrid computation, the decision of the source-visiting set is static, whereas the selection of the testing sequence is dynamic. In particular, a hybrid computation scheme called mobile-agent-based directed diffusion is proposed in [7]. Specifically, if the sources in the target region detect an event of interest, they flood or broadcast exploratory packets to the sink nodes. The whole process is determined by the source-visiting sequence as it migrates among the nodes in the source-visiting set. Therefore, the mobile agent follows a cost-efficient path among target sensors.

Service Traffic

Service traffic contains two aspects: *score* and *form*. The score implies the degree of interest a user has in multimedia traffic, while the form denotes the content features on a particular device. For the purpose of efficiently operating various types of multimedia traffic, we classify the data into three categories: *preference data*, *situation data*, and *capability data*. At first, the multimedia traffic server calculates the similarity between the media service and the preference data by employing the method in [7]. Then it evaluates the probability of the media service belonging to one of the servers. We can get the score from the weighted sum of the above calculated similarity and probability.

Additionally, multimedia traffic adaptation mainly uses two techniques: summarization and transcoding [3]. Multimedia summarization means summarizing a media service into a short one (from the perspective of data size) that can be viewed on a short timescale. Multimedia transcoding means transforming the content from one media type to another so that the content can be suitably processed by a particular device or efficiently transmitted in a specific communication condition.

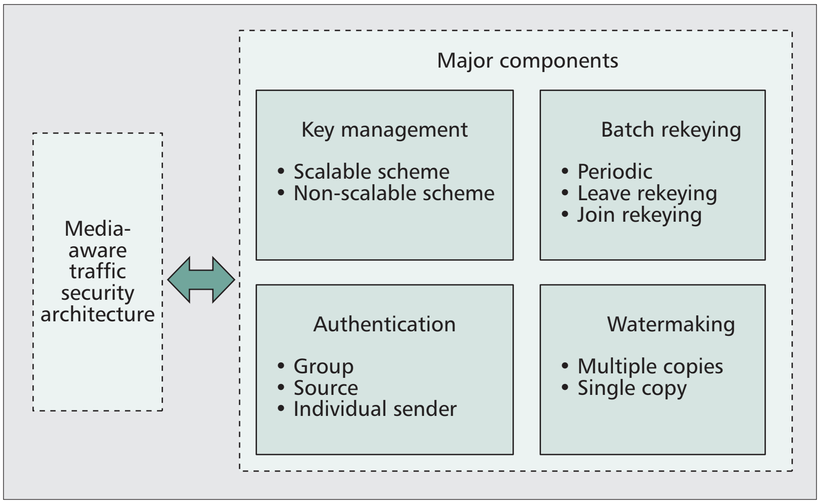

Figure 3. *Major components of MTSA.*

Media-Aware Traffic Security Architecture

In order to meet the information security requirements for multimedia communication, computation, and service in the environment of an IoT, it is necessary to consider some criteria that refer to the traffic security strategy and performance. In this section, we provide a novel media-aware traffic security architecture (MTSA) to solve this problem. It should be noted that MTSA is a development of the information security framework, and multimedia traffic and contents are embedded into the existing architecture [8]. Figure 3 shows the four major components of MTSA.

Key Management

Many network-based key management schemes have been proposed in the last decade, and they can be divided into three classes [7]:

- Non-scalable and scalable schemes. Scalable schemes can also be divided into three groups: *hierarchical key management*, *centralized flat key management*, and *distributed flat key management*.
- Flat schemes, clustered schemes, tree-based scheme,s and other schemes [6].
- Centralized schemes, distributed subgroup schemes, and distributed schemes [5].

We propose a new classification using two criteria: the multimedia traffic that exercises the control and whether the scheme is scalable or not. Thus, we get three classes: *service control*, *user control*, and *flow control*. Each class is further classified into *scalable* and *non-scalable* schemes. In the context of IoT key management, scalability refers to the ability to provide a larger group of multimedia contents without any prior knowledge. A scalable scheme is able to manage a large group over a wide area with highly dynamic sensors. If the computation and communication traffic at the sources increase dramatically with the size of the group, the scheme is treated as non-scalable.

Batch Rekeying

In spite of the efficiency of scalable schemes for multicast applications, changing the key has two major weak points: synchronization and inefficiency [6]. Periodic batch rekeying provides a good trade-off between security improvement and computation complexity. Usually, a new user has to wait longer to join the service group, and the period of batch rekeying is thus a design parameter that can be adjusted according to different security requirements and current network conditions. To accommodate different multimedia application needs, three modes of operation are suggested [9]:

- *Periodic batch rekeying*: The key server handles both join and leave requests periodically in a batch.
- *Periodic batch leave rekeying*: Tthe key server deals with each join request immediately to reduce the delay for a new user to access the IoT but processes leave requests in a batch.
- *Periodic batch join rekeying*: The key server deals with each leave request immediately to reduce the exposure to users who have left but handles join requests in a batch.

Authentication

User authentication involves methods ranging from the use of access control and capability certificates to mutual authentication between the server and user [3, 4].

- *Access control*: The multimedia server maintains a list of hosts who are either authorized to join the service group or excluded from it. When a user sends a join request, the server checks its ID in the access control list to determine whether membership is permitted or not. It is necessary to note that update of this list is important since the list may change dynamically with new authorizations or exclusions.
- *Ability certificates*: Usually, it is issued by a designated certificate authority. An ability certificate contains information about the identity of the host and a set of rights. It is used to authenticate the user and give him/her rights to access multimedia data.
- *Mutual authentication*: The server and user authenticate each other via cryptographic means. From [8], we know that the public key scheme can be used for this purpose.

As we know, multimedia authentication is a challenging problem in secure heterogeneous communications. According to different types of multimedia applications and the network resources available to users, three levels of multimedia authentication can be used:

- *Group authentication*: provides assurance that the packets are transmitted by a registered group member (a registered server or a registered user)
- *Source authentication*: provides assurance that the packets are transmitted by a registered user
- *Individual sender authentication*: provides assurance of the identity of the registered user of the packets

Watermarking

Typical uses of watermarks include *identification of the origin of content*, *tracing illegally distributed copies,* and *disabling unauthorized access to content* [8]. Generally speaking, characteristics and requirements for watermarks in multimedia applications are totally different. Identification of the origin of multimedia content requires the embedding of a single watermark into the content at the server. To trace illegal copies, a unique watermark is needed based on the location or identity of the recipient in multimedia applications. For general delay-sensitive multimedia applications, watermark extraction or detection needs to take place only when there is a dispute regarding a user's rights.

Frankly speaking, the copyright protection problem in the IoT is also a challenging problem. All users in a network group receive the same watermarked content. If a copy of this content is illegally distributed to other users, it may be difficult to find out who is responsible for this action. Such a problem can be eliminated in a homogeneous network environment by embedding a unique watermark for each user.

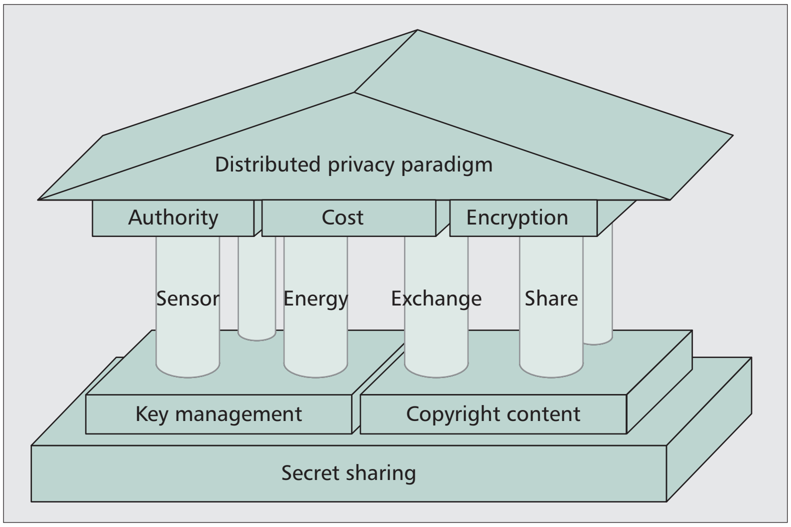

Figure 4. *Design rule and strategy for a distributed privacy paradigm.*

Design Rule and Strategy

MTSA provides a systematic framework for multimedia information security, however, designing the corresponding rule and strategy for MTSA is still a challenging task. The decentralized data acquisition process in MTSA offers opportunities to exploit the distributed nature of the network. We provide a novel distributed privacy paradigm for MTSA, in which the authority, cost, and encryption are obtained in a decentralized manner. Figure 4 illustrates the corresponding general rule and strategy.

Goal and Model

The above discussion motivates us to aim at the following goals for a distributed privacy system:

- Each sensor or mobile agent must create its own share without the need for a central authority.
- From the perspective of size, each secret sharing must not be larger than the original secret.
- From the perspective of an attacker, obtaining multimedia contents will not degenerate the secret sharing size.

Specifically, the first goal makes it necessary to employ a distributed method with traditional service architecture. The second one promotes cost-effective share processing and excludes the method of straightforward encryption. Since each sensor in IoT has correlated information, it is essential that this similarity can be used for reducing the secret sharing size. The third one protects the IoT system from an attacker who may access to the static multimedia contents by reconstructing a secret. In particular, the characteristics of the threat model we employ are as follows:

- Each user can eavesdrop on only a small subset of communication paths.
- Once a node is hijacked, it will be removed from the system.
- An active attack on multimedia applications is performed at normal sensors.

The first threat assumption reflects a reasonable level of capability of the attacker. To reduce the share size, an attacker must be physically distributed across the entire IoT. The second and third threat requirements make it impossible to corrupt the server content during the process of share generation.

Distributed Secret Sharing

The approach we consider is different from the traditional secret sharing problem. In secret sharing, a trusted central authority (sometimes a multimedia server) shares a single secret for many users. Here, unconditional secrecy is achieved through the server's use of hash functions for share generation that are known only to the server; not even the users can access the share.

There are several differences between the secret sharing for MTSA and traditional secret sharing algorithms. First, traditional secret sharing is designed to create shares from a single unique secret. In the case of MTSA, each sensor has a correlated reading of the others representing a composite secret; direct application of secret sharing to each component of the composite secret would be bandwidth-inefficient, making it crucial to design a nontrivial method to account for correlations. Second, given the centralized nature of secret sharing, where a server creates the shares, one straightforward adaptation is to have the sensors in a group exchange their information to a single node. However, given the high possibility of an inside attack, traditional algorithms suffer from a single point of failure. In particular, an attacker just needs to physically compromise the server to eavesdrop. Third, if each sensor can access all the servers, each node would necessarily have to share the random multimedia content with one server, making it again easier for an eavesdropper to obtain the values by compromising any one of the sensors.

According to the above analysis, we develop a new paradigm that is suitable for MTSA. Although secret sharing and visual secret sharing have been proposed for a while, a distributed variant of the visual secret sharing paradigm is our contribution. Our proposed algorithm sacrifices unconditional secrecy to provide a general multimedia security solution for all the sensors in an IoT. In particular, we employ a visual secrecy measure that degrades proportional to the number of shares in possession of an eavesdropper. Such a relaxed definition of secrecy is based on perceived multimedia distortion [5, 7]. Compared to traditional visual secret sharing solutions, the proposed scheme reduces the complexity of multimedia computations and decreases the size of the shares. This point is very important for MTSA. The framework of the proposed paradigm for implementing MTSA is shown in Fig. 5.

Further Discussion

Here, we discuss the possible directions for further developing the proposed distributed secret sharing for MTSA.

- As the key management is an important issue in all encryption based security systems, it cannot be separated from the design of secure multimedia distribution. In most distribution architectures, multimedia content is encrypted with a symmetric key which also needs to be protected in transmission to the user. A common tool of achieving the protection of the decryption key is public-key cryptography. The difficulty in cryptanalyzing public-key ciphers would provide reasonable security for all kinds of multimedia applications [9].
- It is necessary to develop new models that specify how digital copyrighted content can be consumed from the perspective of multimedia service providers in an IoT. The usage rights need to be delivered to the users together with the multimedia content and the decryption keys. The simplest form of this strategy is copy control information (CCI). It expresses the conditions under which a user is allowed to copy multimedia content legally. An important subset of CCI is the two copy generation management systems: "11" (copy-never), "10" (copy-once), "01" (no-more-copies), and "00" (copy-free). It is possible to associate CCI with content in two ways: included

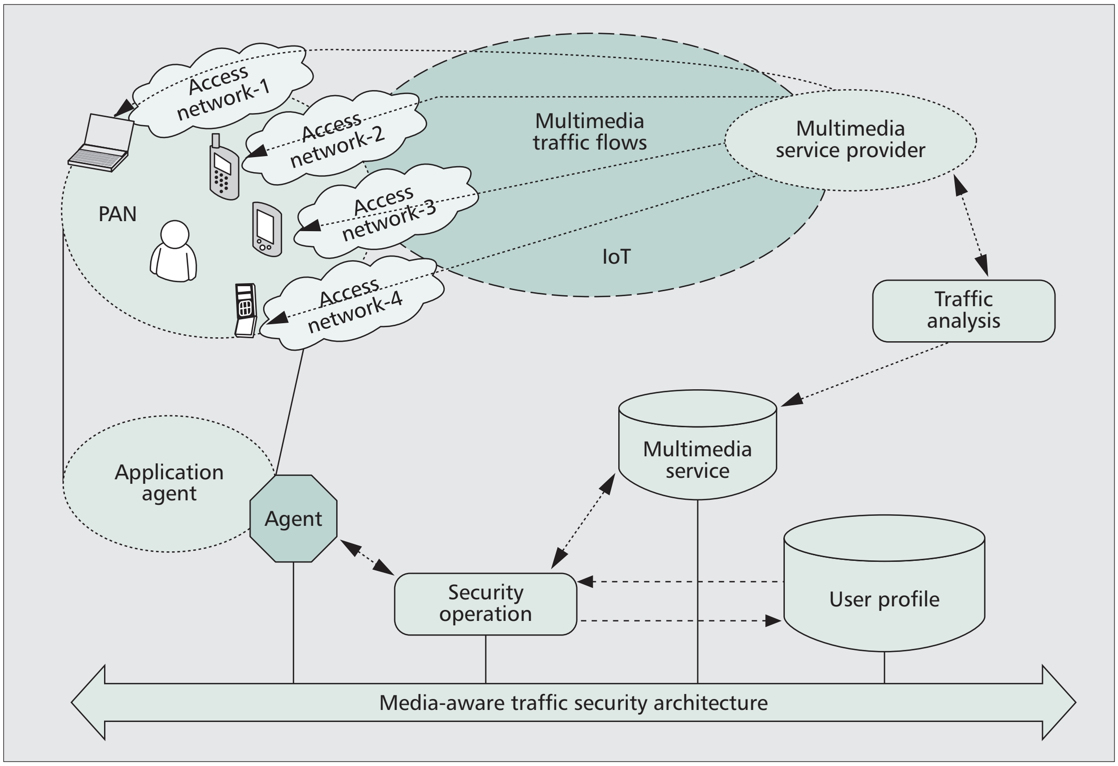

Figure 5. *The framework of the proposed paradigm for implementing MTSA [3].*

in a designated field in a multimedia stream, and embedded as a watermark in a multimedia stream.

Conclusions

In this work, we design a new and efficient media-aware security framework for facilitating diverse multimedia services in internet of things environment. At first, we present the multimedia traffic classification and analysis for handling the heterogeneity of diverse networks. After that, a novel media-aware traffic security architecture is presented based on the proposed traffic classification to enable diverse multimedia services provisioning to users anywhere at any time. At last, we propose the design rule and strategy to achieve a good trade-off between system flexibility and efficiency.

Acknowledgment

This work is supported in part by the National Science Council, Taiwan under Grant NSC 99-2219-E-197-001 and Grant NSC 99-2219-E-197-002.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, Oct. 2010, pp. 2787–805.
[2] M. Chen, S. Gonzalez, and V. Leung, "Applications and Design Issues of Mobile Agents in Wireless Sensor Networks," *IEEE Wireless Commun.*, vol. 14, no. 6, 2007, pp. 20–26.
[3] L. Zhou *et al.*, "Context-Aware Multimedia Service in Heterogeneous Networks," *IEEE Intelligent Sys.*, vol. 25, no. 2, Mar./Apr. 2010, pp. 40–47.
[4] L. Zhou *et al.*, "Distributed Scheduling Scheme for Video Streaming over Multi-Channel Multi-Radio Multi-Hop Wireless Networks," *IEEE JSAC*, vol. 28, no. 3, Apr. 2010, pp. 409–19.
[5] H. V. Zhao, W. S. Lin, and K. J. R Liu, "A Case Study in Multimedia Fingerprinting: Behavior Modeling and Forensics for Multimedia Social Networks," *IEEE Sig. Proc. Mag.*, vol. 26, no. 1, Jan. 2009, pp. 118–39.
[6] M. Chen *et al.*, "Software Agent-based Intelligence for Code-centric RFID Systems," *IEEE Intelligent Sys.*, vol. 25, no. 2, Mar./Apr. 2010, pp. 12–19.
[7] D. Kundur *et al.*, "Security and Privacy for Distributed Multimedia Sensor Networks," *Proc. IEEE*, vol. 96, no. 1, Jan. 2008, pp. 112–30.
[8] A. M. Eskicioglu, "Multimedia Security in Group Communications: Recent Progress in Key Management, Authentication, and Watermarking," *Multimedia Systems*, vol. 9, 2003, pp. 239–48.
[9] H. Susanto and F. Muhaya, "Multimedia Information Security Architecture Framework," *Proc. FutureTech 2010.*

Biographies

LIANG ZHOU [M] (liang.zhou@ieee.org) received his Ph.D. degree in electronic engineering from both Ecole Normale Superieure, Cachan, France, and Shanghai Jiao Tong University, China, in March 2009. From 2009 to 2010 he was a postdoctoral researcher at ENSTA-ParisTech, France. Since October 2010 he has been a Humboldt Research Fellow at the Technical University of Munich, Germany. His research interests are in the area of networked multimedia communications and computing.

HAN-CHIEH CHAO [SM] (hcc@mail.niu.edu.tw) is a joint appointed full professor of the Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University, Taiwan. His research interests include high-speed networks, wireless networks, IPv6-based networks, digital creative arts, and the digital divide. He currently serves as Editor-in-Chief for *IET Communications*, *International Journal of Ad Hoc and Ubiquitous Computing*, *Journal of Internet Technology*, and *International Journal of Internet Protocol Technology*. He is a Fellow of the Institution of Engineering and Technology (FIET) and a Chartered Fellow of the British Computer Society (FBCS).