Published in IET Information Security
Received on 10th December 2009
Revised on 19th March 2010
doi: 10.1049/iet-ifs.2009.0261

Special Issue on Multi-Agent & Distributed Information Security

ISSN 1751-8709

Survey of security services on group communications

P. Sakarindr N. Ansari

Advanced Networking Laboratory, Electrical and Computer Engineering Department, NJIT, University Heights, Newark, NJ 07102, USA
E-mail: ps6@njit.edu

Abstract: Secure group communication (SGC) has attracted much attention, as group-oriented communications have been increasingly facilitating many emerging applications that require packet delivery from one or more sender(s) to multiple receivers. Of all proposals reported, most have focused on addressing the issue of key management to SGC systems. The authors, however, advocate that security services are also needed to satisfy different security requirements of various applications. The authors also present here a survey on recent advances in several security requirements and security services in group communication systems (GCSs), illustrate some outstanding GCSs that deploy these security services, and describe challenges for any future research works in designing a secure GCS.

1 Introduction

Group communication refers to either point-to-multipoint or multipoint-to-multipoint communications via some underlying networking infrastructures. In this article, we do not specify the underlying networking infrastructures to support group communication systems (GCSs), since there are currently no concrete works or standards on those networks to effectively secure group communications. However, we will describe the ongoing activities of the IETF multicast security charter work group (IETF MSEC WG) to standardise the multicast security framework and architectures for internet protocol (IP)-based multicast networks.

Different security services may be needed to satisfy different security requirements for different applications. This article discusses the following six security requirements in group communications: group authentication, group authorisation and access control, group accountability and non-repudiation, group privacy and anonymity, group message integrity and confidentiality and group survivability and availability. These requirements can be achieved mutually or independently by five security services, including group key management (GKM), group access control, group anonymity, group signature and secure routing. The most fundamental component of security services is the cryptographic material, such as keys. Thus, the performance of security services inherently relies on the strength and security of the cryptographic material. Many proposals developed so far for SGCs systems have mainly focused on solving the issues of key management. However, this article aims to demonstrate that any SGCs system should offer as many security services as feasibly possible. The readers are further referred to [1] for a survey on SGCs in wireless networks, such as mobile *ad hoc* networks and wireless sensor networks, for a broader understanding of SGCs.

The rest of the article is organised as follows. Security requirements and services in group communications are discussed in Section 2. Attributes for evaluating each security service and a comparison of these attributes are presented in Section 3. Some outstanding GCSs are then reviewed in Section 4. Some existing group communications-oriented networks are illustrated in Section 5. Finally, we present the challenges ahead and summarise the article in Sections 6 and 7, respectively.

2 Security requirements and services for group communications

This section describes security requirements for group communications, which are also the basic security

requirements for most network communications. Security services that meet these requirements are depicted in Fig. 1 and are elicited separately later in the subsequent section.

Group authentication: It enables a group member to be authenticated as unspecified, but a legitimate member, such that the sending member can multicast a message on behalf of the group without revealing its identity during the verification process performed by the receiver. Besides user authentication, message authentication allows any group message to be verified for its authenticity.

Group authorisation and access control: Every member may be assigned the same or different permissions and restrictions for accessing group resources. The access-controlling entity can verify a member's request to access specified resources by using several means, such as the access control list and access hierarchy.

Group accountability and non-repudiation: All group operations should be accountable, implying that any group operation performed and resources utilised can be tracked and recorded in order to detect any abusing usages of resources and operations. A non-repudiation requirement ensures that the identity of a member whose activities are in dispute can be fully and precisely identified by the designated entity.

Group privacy and anonymity: Fundamentally, group privacy and anonymity contradict to group accountability and non-repudiation because the privacy of a malicious group member should be stripped off and its identity should be exposed. There have been some researches trying to determine the trade-offs between these requirements. For example, some threshold sharing mechanisms may allow a number of designated entities to gather information and to recreate some secret elements used to ultimately identify the wrong-doing members.

Group message integrity and confidentiality: Message integrity should be preserved by ensuring that the message has not been added, deleted or modified by any unauthorised entity, either unauthorised members or outsiders. In GCSs, the integrity is ensured by encrypting a group message with a single shared key, called a group key. Thus, the message protection mainly relies on the cryptographic strength of the group key. Confidentiality ensures that only the authorised can retrieve meaningful data from the message.

Group survivability and availability: An attacker may attack multicast routers and other routing infrastructures or target a joining operation in order to cut off some or all group members or to disrupt group communications, thus causing service unavailability. To achieve group survivability, the routing protocol should ensure that any member can still be connected even under attacks. Furthermore, there should be some preventive mechanisms to support group survivability by rediscovering connections in the events of link or node failures.

3 Performance attributes to evaluate secure GCSs

In order to evaluate and compare different SGC systems, one needs to construct evaluation attributes to fairly analyse and determine the performance and security analysis of each

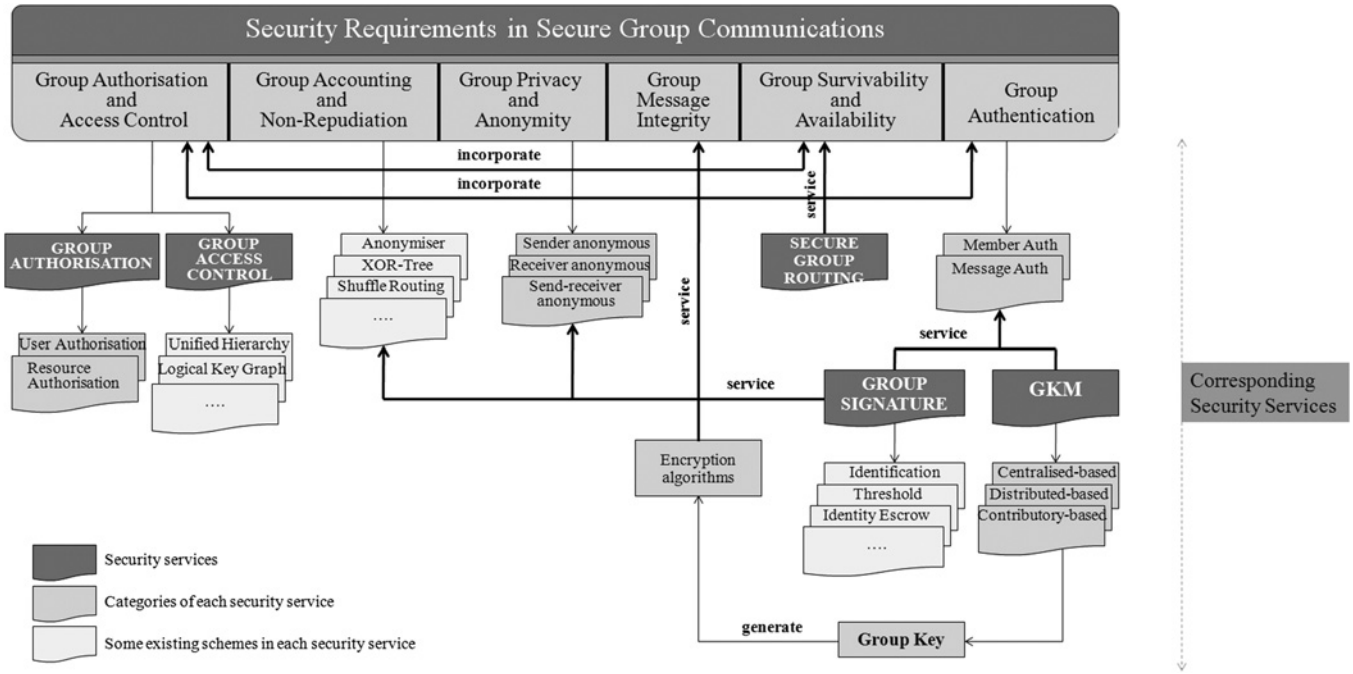

Figure 1 *Security services correspond to security requirements*

SGC system. In this article, evaluation attributes are grouped into two types: fundamental attributes used to evaluate mechanisms in providing one or more security services to GCSs and specific attributes used as additional properties corresponding to those supported security services.

3.1 Fundamental attributes

The fundamental attributes for a SGC system may include the following as depicted in Fig. 2.

Types of group management: The group may be established and managed by three approaches: centralised (with a central authority), partially distributed (with a group of designated controllers) and fully distributed (without any explicitly designated controller). The group controller may perform the group initiation and termination, the membership admission, the group material generation and the distribution of some controlling messages. The group controller may also act as a key server, if given the capacity.

Overheads: In general, three types of overheads are incurred by all network operations: storage, communications and processing. For storage overheads, a group controller and a group member may require different amounts of memory to store group information such as session and group keys, list of group members, cryptography materials and other service-related materials. For communications overheads, the characteristics of group communications likely incur additional communications messages. For example, dynamic group membership changes cause members to reorganise group operations (i.e. sending joining or leaving notifications, selecting new group controllers) and to rekey all related keys to ensure key secrecy (i.e. distributions of new keys). To process overheads, each group operation requires computation which can be measured in terms of the number of processing steps (iterations), processing duration and complexity bound. The key generation and distribution, rekeying and message encryption/decryption/digestion/signing processes are computationally expensive.

Scalability: The performance should not be degraded drastically as the group size increases; it should be linear with the group size. In addition, the scalability may be increased in many scenarios: for example, a group is managed in a distributed approach (because of easiness to expand the group).

Dynamic membership: GCSs should be able to handle a membership change (i.e. any individual member leaves or joins the group at any time) without significant system performance degradation. Some systems may treat groups merging and partitioning the same way as a bulk of individual membership changes, and may thus suffer from degraded performance when handling a large group of membership changes. Different networks may handle the group membership changes differently. For example, wireless *ad hoc* networks may observe higher mobility of members (more frequent membership changes), whereas multicast wired networks may expect less or even fixed mobility (less frequent membership changes).

Trust relationship: Some systems require a trusted third party such as the certificate-issuing authority and the key server, which can make the trusted third entity a point of attack. Some systems assume trust relations among group controllers or between a group controller and members, but ignore the need for additional security mechanisms to protect trust operations such as trust establishment and updating trust relations.

Resilience: It is necessary to include a threat model and the security analysis in designing and evaluating a SGC system. To analyse the threat model and security analysis, both

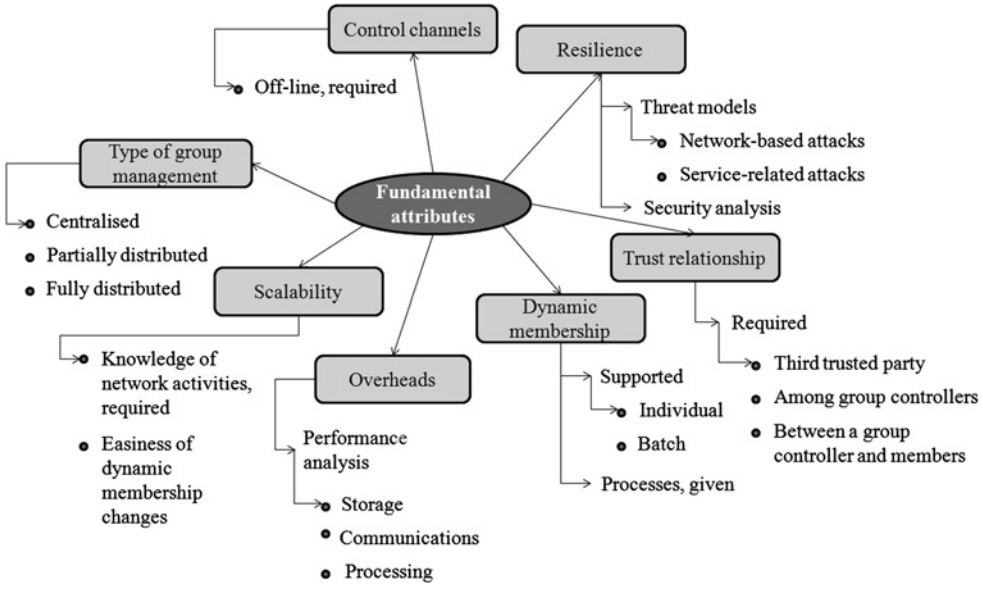

Figure 2 *Fundamental attributes for evaluating performance and security in a SGC system*

doi: 10.1049/iet-ifs.2009.0261

network-based attacks and service-related attacks are considered. The network-based attacks are general attacks that explore the vulnerabilities of a network. The service-related attacks specifically target the security service mechanisms originally deployed to satisfy some security requirements. For example, a group signature satisfies privacy and authentication, but unintentionally, leaves the SGC system with new vulnerabilities, such as weaknesses in the signature algorithm or erroneous source codes in generating the signatures. The security analysis may be able to detect and prevent such vulnerabilities.

Control channels: Some systems require offline communications channels, such as using a telephone or control channels. The performance and security analysis should measure online impacts of the offline channel.

3.2 Service-specified attributes

Additional properties or attributes for specific security services are discussed separately as depicted in Fig. 3.

3.2.1 Group key management: A GKM scheme should exhibit the following six additional properties:

Types of key management: In a centralised key management, a key manager generates the keys, distributes them to associated members and maintains all the keys. The security of key generation is strong, but the key manager carries most of the workloads and becomes the attack target. In a partially distributed key management scheme, a set of key managers generate the keys and distribute them to all group members. Thus, each key manager has a reduced workload. Each key manager may still become the attack target, and the security of key generation is weakened. In a contributory key management scheme, each member randomly selects its contribution, exchanges within a group and generates a shared group key without a central key server/manager. The security of key selection and generation is low, but there is no need for a key manager. All members equally share the workloads.

Key secrecies: There are three aspects of key secrecies: forward secrecy, backward secrecy and perfect forward secrecy. The forward secrecy ensures that a new joining member cannot use the new key to decrypt all messages which have been encrypted with the previous key(s). The backward secrecy ensures that a leaving member cannot use the previous key(s) to decrypt all messages encrypted with

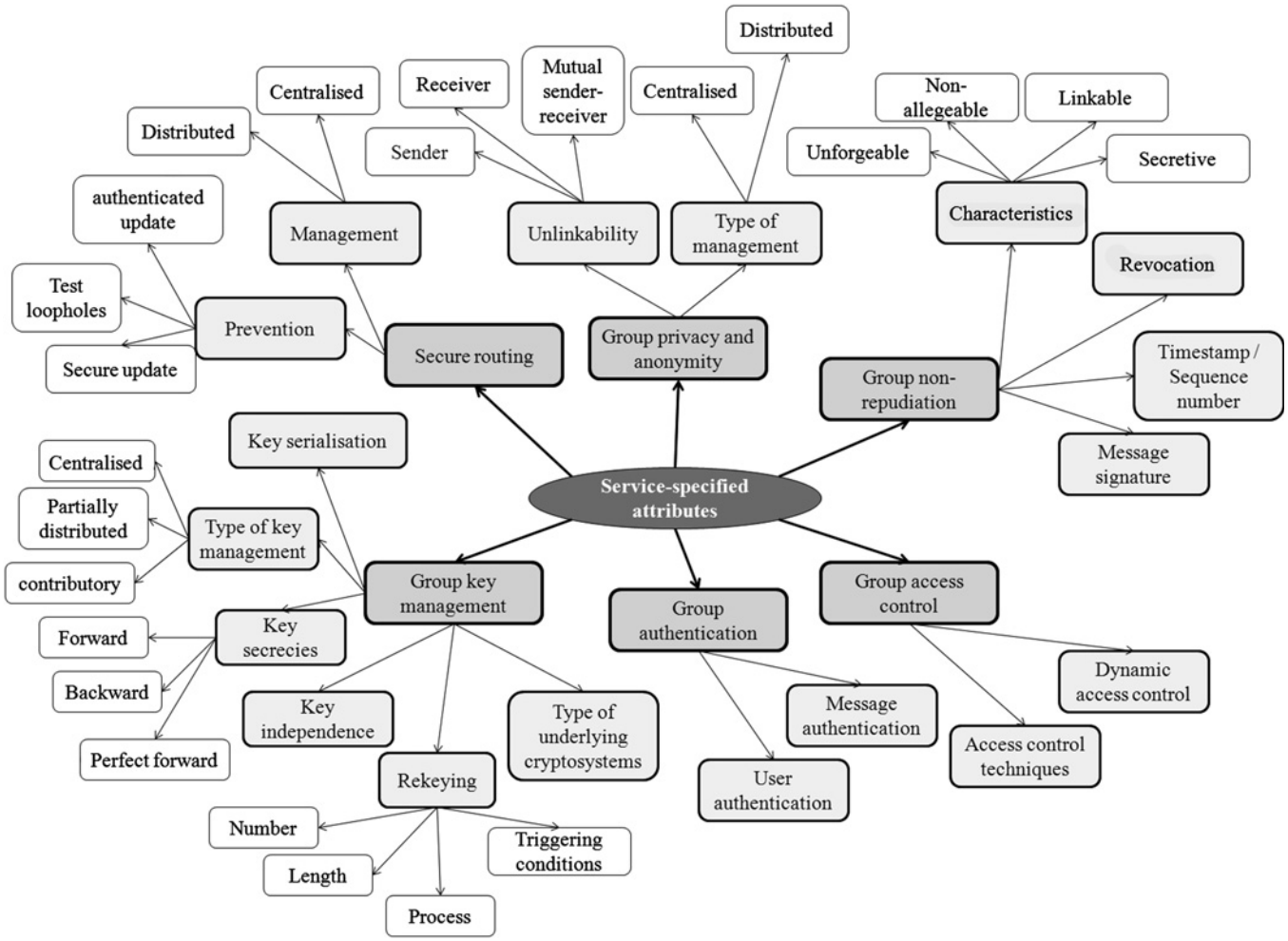

Figure 3 *Service-specified attributes for evaluating security services in a SGC system*

the new key. The perfect forward secrecy ensures that a compromise of a long-term key seed that generates the present short-term key(s) cannot deprive the secrecy of other previous short-term keys which have been generated by the compromised long-term key.

Key independence: A disclosure of a subset of session keys cannot deprive the secrecy of other subsets of session keys which have been generated by the same long-term key seed.

Key serialisation: The key materials are selected and the group key is generated by members in an ordered sequence. An attack on any participating member disrupts the whole process. Instead, some schemes may construct the key by other means; that is, broadcasting the key materials or establishing a key tree, at the expense of overheads.

Rekeying: There are several factors in evaluating rekeying as follows: (i) The number of rekey messages – the number of distributed and received messages per member or per key manager may be different; (ii) The length of rekey messages – some protocols aggregate multiple rekey messages into a single message, which in return increases the consumed bandwidth for one transmission. Thus, the performance analysis should also determine the bandwidth consumption per message in addition to the number of transmitted messages; (iii) The rekeying process – the rekeying operation should reduce or optimise the computation and time complexity of the rekeying operation with respect to a group size; (iv) Triggering conditions – there are three scenarios: first (rekeying based on membership changes), keys associated with the membership changes must be rekeyed to ensure the key secrecy for the remaining members; second (periodic rekeying), the rekeying operation is invoked periodically to prevent keys from being compromised over time and third (specified rekeying), a system enables the rekeying operation for specified incidents, such as upon detection of attacks or violations.

3.2.2 Group access control: The following two additional properties related to a group access control scheme are considered:

Access control: The group resources and group messages should be accessible only to authorised members.

Dynamic access control: The system enables its members to dynamically change their request to access resources. Consequently, the system must be able to update access permissions and restrictions with additional mechanisms when a member's access privilege changes.

3.2.3 Group signature: Three additional properties related to a group non-repudiation scheme are considered:

Message signature: A system requires messages to be signed with a membership certificate to identify the originator (signer) of the message.

Timestamp or sequence number: Timestamps and/or sequence numbers can be used to limit the validation of a certificate or message signature in order to prevent replay attacks.

Revocation of certificates: The expired certificate or misuse of a certificate should be revoked by the issuer, and publicly announced in the revocation list. Some systems may keep the expired certificates for future verification at the expense of additional storage overhead.

Characteristics of a signature: There are four basic requirements of a digital signature: (i) unforgeable – a group of colluded attackers cannot generate a group signature identical to that generated by a legitimate member; (ii) non-allegeable – a group of colluded attackers cannot generate a group signature by which a group controller falsely identifies a legitimate member as an attacker; (iii) linkable – a group of colluded attackers cannot generate a valid group signature by which a group controller cannot identify the identity of any of these attackers; and (iv) secretive –a member's secret elements can neither be retrieved from a group signature nor from any part of the signature.

3.2.4 Group anonymity: Two additional properties related to the group privacy and anonymity scheme are considered:

Unlinkability of anonymous communications: There are three anonymities: sender anonymity – a sender shall not be linked to its sent message to prevent attackers from learning of the message's origin; receiver anonymity – a receiver shall not be linked to the received message to prevent attackers from learning of the message's destination and sender–receiver anonymity – the sender and receiver shall not be linked together, and they are also relatively anonymous to each other.

Types of management: There are two types of management: centralised management – a system relays messages through a trusted anonymous entity to hide identities of the sender and receiver and distributed management – a system relays messages through a group of anonymous entities or hides the identities by other means such as encapsulating messages and coding with the XOR operation.

3.2.5 Secure routing: Two additional properties related to a secure routing scheme are considered:

Management: A system can establish and maintain routing-related information in a centralised or distributed manner.

Prevention: Updating routing information must be restricted to authorised members. A new routing path should be tested to prevent routing black hole and loopholes. Any request to join/add/update the routing table and other

IET Inf. Secur., 2010, Vol. 4, Iss. 4, pp. 258–272
doi: 10.1049/iet-ifs.2009.0261

routing-related information should be authenticated and authorised.

We shall next compare existing outstanding secure GCSs in terms of the properties discussed above. The results are summarised in Tables 1 and 2, in which shaded boxes in Table 2 indicate that the security services are irrelevant to the systems and are thus excluded from consideration.

4 Security services for group communications

This section discusses essential security services that meet security requirements mentioned before. Many concepts and existing solutions have been proposed to provide such services, but only a few promising concepts and solutions are highlighted here owing to the space limit.

4.1 Group key management

Any GKM scheme should exhibit the following properties: the key generation and rekeying should be provably secure; an imitation of the group key should be mathematically infeasible or computationally difficult; the group key is securely distributed and only the legitimate users can obtain a valid group key and a revocation of the group key upon a membership change should be immediately notified.

Banerjee and Bhattacharjee [2] proposed a management scheme based on a clustering protocol and a hierarchy of keys. All members are divided into several clusters in a layer. In each cluster, a cluster header will be selected and be a cluster member of the upper layer. This process is repeated until there is only one cluster member in the top layer. The clustering protocol is deployed to cluster the members in each layer such that when a membership changes, only one cluster in each layer requires its associated keys to be updated. It was demonstrated that, for an individual membership change, the overheads incurred by group members are constant with respect to the group size. In addition, for a bulk membership change, the processing and communication overheads at the key server are logarithmic with respect to the group size.

Wong *et al.* [3] introduced three-key graph-based rekeying approaches (user-, key- and group-oriented) to mitigate the scalability problem. In events of membership changes, three rekeying approaches operate as follows: for user-oriented rekeying, the key server generates new keys for each affected member and encrypts them with keys previously held by that member; for key-oriented rekeying, the new keys are encrypted individually with previous keys at the same key nodes of the key tree and multicast in multiple rekey messages and for group-oriented rekeying, it is similar to the key-oriented rekeying except that all new keys are put together in a single rekey message. The simulation results demonstrated that the complexities of rekeying overheads of the three approaches are linear with the logarithm of the group size. In addition, the group-oriented approach performs the best from the perspective of the key server, whereas the user-oriented approach has the best performance from the perspective of the group member.

Amir *et al.* [4] secured group communications with a secure service from the proposed robust and contributory key agreement protocol and the virtual synchrony semantics. The proposed protocol enhances the group Diffie–Hellman key agreement in two ways: first, it can mitigate the member serialisation problem that requires the group key to be constructed or rekeyed in a serial ordering; second, it incorporates a membership protocol such that it is aware of any membership changes during the key generation and rekeying processes. In addition, the proposed protocol can effectively handle events of members joining and leaving within a very short time interval. Their simulated system, called secure spread, demonstrated the reduction of time used to successfully establish a secure group and generate a group key after a membership was changed.

4.2 Group access control

In group-oriented networks, group members can be assigned with multiple access privileges. The data stream can be accessed with different access privileges such that only members who have an appropriate privilege can access to corresponding portions of contents of the data stream (or some data streams of the aggregated data stream). This is referred to as multiple access privilege. In addition, some GCSs can support dynamic access control.

Sun and Liu [5] proposed multi-group (MG) key management scheme to construct the logical key graph by integrating key trees of all members. Each authorised member holds a set of keys associated with the nodes from the leaf node to the root node in the key graph. The access privilege for each member is determined by the possessed set of keys. The scheme can provide forward and backward secrecies when a member changes its access privileges (or leaves the group) because the set of keys and resources associated with that member are reassigned (or withdrawn). It was shown that overheads caused by the rekeying incidents are greatly reduced. In addition, the scalability and complexity of the scheme is improved.

Zhang and Wang [6] proposed a hierarchical access control (HAC) key management scheme, where a key server maintains the description of relations of memberships and resources in the form of unified hierarchy. Instead of classifying members with different resource requirements into multiple groups as of the conventional multi-group (MG) key management scheme, the HAC scheme constructs a membership-group sub-graph and a resource-group sub-graph, and combines them into a single unified logical key graph that determines which resource the specified member can access. The simulation results have demonstrated that, with the HAC

Table 1 Comparison of secure GCSs along with fundamental performance properties

Services		Group key management			Group access control		Group signature		
Evaluation properties		Ref [3]	Ref [4]	Ref [5]	Ref [6]	Ref [7]	Ref [8]	Ref [9]	Ref [10]
type of group management		partially distributed (an authentication and access control server + cluster leaders)	distributed (subgroups)	distributed (logical servers)	centralised (with a key distribution center) + contributory scenarios	any (with a key server)	centralised (a group manager)	centralised (with a shadow distribution centre)	centralised (a group manager)
reduction of storage overheads		yes	yes	no	yes	yes	no	only one secret kept at each member	no
reduction of communication overheads		yes	yes	yes	N/A	N/A	no	no	no
reduction of processing overheads		yes	yes	yes	yes (for rekeying)	yes (for rekeying)	no	no	no
performance is steady with a group size		yes	yes	yes	yes	possible but not clearly stated	N/A	N/A	N/A
scalability supported		yes	yes	yes	yes	possible but not clearly stated	no	no	no
Dynamic membership	individual change	yes	yes	yes	yes	yes	yes	no	no
	a bulk of changes	yes	no	yes	no	no	no	no	no
trust among group entities required		yes (among members)	yes (for key server(s))	no	no	no	no	no	yes (for the verifier(s))
message integrity methods		N/A	session key	group key	session key and key-encrypted keys	data encryption keys (resource and membership-group keys)	N/A	N/A	N/A

Services	Anonymity		Secure multicast routing	
Evaluation properties	Ref [11]	Ref [12]	Ref [13]	Ref [14]
type of group management	centralised (a group authority and a group controller)	fully distributed	partially distributed (sub-branch core routers, and an authentication service)	partially distributed (domain core routers + a center router)
reduction of storage overheads	yes	no	no	no
reduction of communication overheads	yes	yes	no	no
reduction of processing overheads	yes	yes	no	no
performance is steady with a group size	no	yes	no	no (for edge/ core/ center routers)
scalability supported	yes	unlikely but not clearly stated	yes (for key generation and management) no (for rekeying)	yes

Continued

IET Inf. Secur., 2010, Vol. 4, Iss. 4, pp. 258–272
doi: 10.1049/iet-ifs.2009.0261

Table 1 *Continued*

Services		Anonymity		Secure multicast routing	
Evaluation properties		Ref [11]	Ref [12]	Ref [13]	Ref [14]
Dynamic membership	individual change	N/A	N/A	yes	yes
	a bulk of changes	no	no	no	no
trust among group entities required		no	no	yes	no
message integrity methods		message encryption and session keys	pseudorandom sequences	random encryption keys + branch keys	hash of encrypted messages + domain control key + group data key + sender specific keys

scheme, the storage and rekeying overheads at every member and the key server can be significantly reduced by at least 20% as compared with those of the MG scheme.

4.3 Group signature

The group signature is used to authenticate the source whether the message is sent from the signer who is a legitimate, but unidentified, group member and to authenticate the message whether it has been altered during transmission. In case of a dispute, the third trusted party or the group controller can identify the actual signer of the signed message.

Chen *et al.* [7] proposed a scheme that combines a provably secure scheme and identification (ID)-based scheme to provide authentication, anonymity and non-repudiation. Unlike the original ID-based signature scheme, the proposed scheme generates a member's public key from its identity information (e.g. e-mail address, name, network address, etc.). As an advantage to the scheme, the group controller uses the smaller ID rather than the larger public key, as used by a public key infrastructure-based scheme, to generate a member's private key in order to reduce the storage overhead. A member signs the message with its private key on behalf of the group.

Lee [8] proposed a threshold signature scheme with multiple signing policies. The scheme enables the group signature-generating functionality to be shared among at least any t members out of n members, so that a threshold value of the signature is t. Any $t-1$ or lower members cannot generate or reconstruct the same signature with the threshold value of t. This proposed scheme demonstrated that each user stores only a group secret key (called a public shadow), thereby significantly reducing the storage and communication overheads for group signature generation.

Ateniese *et al.* [9] proposed a provably secure group signature scheme and a modified identity escrow scheme. The proposed scheme enables a group member to authenticate the new comers by using the zero knowledge proof method before issuing a membership certificate. In addition, the scheme allows group members to perform group signing by showing the proof of knowledge of their certificates. Using a modified identity escrow scheme, the receiver is not aware of the signer's identity but is guaranteed by the third trusted verifier that the signer's signature can be opened and linked to the signer. Thus, a signer does not expose its secret to the verifier during the verification process. Furthermore, the scheme is provably coalition-resistant against an adaptive attacker who can adaptively run the joining process as multiple new members in order to obtain sufficient information to generate valid group certificates.

4.4 Group anonymity

Many articles have proposed solutions to provide anonymity in unicast communications, but these solutions may not be suitable for group communications in the following ways: (i) a node has to hide from multiple nodes; (ii) group membership management becomes challenging for providing anonymity; (iii) an extremely complicated GKM is needed to anonymously generate, distribute and manage multiple keys, including the group key and other keys-protected keys, so that anonymity in group communications can be possibly preserved.

The following schemes attempt to provide anonymity in group communications: Xiao *et al.* [10] proposed the mutual anonymous multicast protocol that allows communications among three types of nodes: anonymous member (AM), non-anonymous member (NM) and middle outsider (MO) nodes. Initially, a set of NM nodes form the anonymous multicast tree. Then, an AM node sets up connections with three possible choices: NM nodes on the tree that can still accommodate connections – called unsaturated NM nodes, unsaturated AM nodes on the tree and MO nodes that are invited to join the tree. The protocol combines the well-known reverse onion protocol [11] and crowd protocol [12] in the following ways. Each AM node creates a remailer as a list of intermediate nodes whose identities are encrypted with

Table 2 Comparison of secure GCSs along with additional performance properties

Evaluation properties	Group key management-based systems			Group access control-based systems		Group signature-based systems		
	Ref [3]	Ref [4]	Ref [5]	Ref [6]	Ref [7]	Ref [8]	Ref [9]	Ref [10]
key management								
structure of keys	hierarchical cluster-based	key graph	typical group key agreement	tree-based Multi-group key graph	logical key graph			
type of cryptosystem used	DL	RSA	DL and RSA	N/A	N/A			
forward secrecy	yes	yes	yes	yes	yes			
backward secrecy	yes	yes	yes	yes	yes			
perfect forward secrecy	N/A	N/A	yes	N/A	N/A			
key serialisation	no	no	no	no	no			
key independence	yes	yes	yes	N/A	N/A			
rekeying	membership changed	membership changed	membership changed	membership and access privilege changed, and periodic	membership changed			
key management	centralised (a key server)	centralised (a key server)	contributory	centralised (a key distribution centre)	centralised (a key server)			
authentication								
user authentication	yes (auth. list + credential.)	yes	no			yes (membership cert. + zero-knowledge proof)	no	yes (membership cert. + zero-knowledge proof)
message authentication	no	yes	yes			yes (group signing keys)	yes (group secret keys)	N/A
access control								
authorisation/ access control	yes	yes (access control list)	no	yes (hierarchical access control)	yes (hierarchical access control)			
dynamic access control	no	no	no	yes	no			
signature								
message signature	no	message digest	message signature			ID-based group signature	threshold-based group signature	group signature
non-repudiation	N/A	unforgeable and linkable	unforgeable and linkable			unforgeable, non-allegeable, and linkable	unforgeable, non-allegeable, and linkable	unforgeable, non-allegeable, and linkable

Continued

doi: 10.1049/iet-ifs.2009.0261

Table 2 *Continued*

Evaluation properties	Group key management-based systems			Group access control-based systems		Group signature-based systems		
	Ref [3]	Ref [4]	Ref [5]	Ref [6]	Ref [7]	Ref [8]	Ref [9]	Ref [10]
anonymity								
anonymity supported						yes	yes	yes
unlinkability of anonymous communications						sender	sender	sender
type of anonymity management						N/A	N/A	N/A
secure routing								
management								
prevention								

Evaluation properties	Anonymity-based systems		Secure multicast routing-based systems	
	Ref [11]	Ref [12]	Ref [13]	Ref [14]
key management				
Structure of keys			hierarchical branch-based tree	hierarchical domain-based tree
type of cryptosystem used			N/A	RSA
forward secrecy			yes	yes
backward secrecy			yes	yes
perfect forward secrecy			N/A	N/A
key serialisation			no	no
key independence			N/A	N/A
rekeying			membership changed and periodically changed	membership changed
key management			partially distributed (sub-branch routers)	partially distributed (domain routers)
authentication				
user authentication	Possible but not clearly stated	no	yes (certificate)	yes
message authentication	yes	no	yes	yes
access control				
authorisation/ access control	yes (access control cert. and list + access control anonymiser)	no	yes (access control list.)	yes (an authorisation service + access control list)
dynamic access control	no	no	yes	no
signature				
message signature	messages signature	no	digital signature	no

Continued

Table 2 *Continued*

Evaluation properties	Anonymity-based systems		Secure multicast routing-based systems	
	Ref [11]	Ref [12]	Ref [13]	Ref [14]
non-repudiation	N/A	N/A	N/A	N/A
anonymity				
anonymity supported	yes	yes	no	no
unlinkability of anonymous communications	sender-receiver	sender, receiver and sender-receiver		
type of anonymity management	centralised (anonymisers)	distributed		
secure routing				
management			partially distributed (sub-branches)	partially distributed (domains)
prevention			unauthorised modification prevention	unauthorised modification prevention

N/A stands for 'not applicable' or 'no available information'
If a system design does not offer some security services, the corresponding table cells of these security services are emptied and shaded

their associated public keys in layers, similar to layers of an onion. The NM nodes on the tree keep all remailers associated with a particular AM node. The packet originated from or destined to an AM node will be forwarded through the remailer associated with this AM node. For the AM-to-NM connections, an intermediate node chooses either to deliver the packet directly to the NM node or randomly forward the packet to another node, according to the predefined forwarding probability. For the AM-to-AM connections (mutual anonymous connections), the AM 1 node will select one of its middle nodes to establish a connection with one of AM 2's middle nodes.

Grosch [13] provided both sender and receiver anonymity to multicast traffics through both dedicated and shared anonymisers. The anonymiser receives messages from a sender, processes the messages (for the purposes of integrity, confidentiality and anonymity) and forwards them as its own messages to receivers via a secured multicast channel. The scheme determines the location of the anonymiser on the multicast tree in such a way that the network loads and average distance (i.e. the average number of links) from the anonymiser to all receivers can be optimised. To find such an optimal location, the scheme first selects a candidate node in the undirected graph. Then, it assigns the weight of each link on the graph as the number of all receivers that are connected downstream. Based on the link weights, the shortest paths from the candidate node to all receiving nodes are determined, and the multicast tree is formed. To reduce the network load, all nodes can be grouped in a smaller group size, although fewer nodes can then be selected as anonymisers. Given the specified pair of the candidate node and group size value, the scheme calculates the overall weight for this multicast tree as the sum, over all links, of the probability that each link is used. Repeat the process for all combination of candidate nodes and group size values. The node with the lowest overall weight is selected as the anonymiser.

Dolev and Ostrovsky [14] proposed the XOR tree-based scheme to provide efficient anonymous multicast (either sender anonymity, receiver anonymity or both) and to protect the multicast network against the traffic analysis and collusion attacks. The idea is that a forwarding member performs an XOR operation bit-by-bit on data stream forwarded to its predecessor with pseudo-random stream in order to hide the true bits of the data stream. It is analytically demonstrated that the communication overhead on each link and the computational overhead incurred at any member on the forwarding path is greatly reduced.

4.5 Secure routing

In this service, the IP-based multicast network is mainly considered. A single packet is delivered through multicast routers to a large group of receivers. If an attacker can join a multicast group and launches either passive or active attacks, these attacks would effectively incur high overheads and network-wide failures and unavailability.

Unfortunately, many GCSs assume that the group routing structure (e.g. multicast tree) is secure and unauthorised users neither send nor receive the messages. However, a few secure group routing schemes have been proposed to safeguard the routing infrastructures physically and logically. Several

doi: 10.1049/iet-ifs.2009.0261

SGC-based networks illustrate the implementation of security services in various group communications.

Shields and Aceves [15] proposed a keyed hierarchical multicast routing protocol (KHIP) that allows only authorised and trusted members with proper privileges to access and update the multicast tree and prevents unauthorised users from joining or expanding the multicast tree. Data messages are protected with random encryption keys and branch keys, but there is no shared group key for the entire multicast group. A member who serves as the core for each branch reprocesses all passing messages at their origin before forwarding to the parent and children branches of the multicast tree. It was demonstrated that a minimal number of nonces are added to the headers of data and routing updated messages to prevent the replay attack and the forgery attack. Furthermore, the impact of denial-of-service attacks undertaken by untrusted members (e.g. untrusted multicast routers) could be minimised.

Shim [16] introduced a secure multicast routing protocol based on intra-domain and inter-domain routing protocols. The network is divided into domains, each managed by a core router, and all controlling messages associated with the domain are encrypted with a domain control key. All domains are managed by the centre router in a hierarchical tree manner. A non-member user is only able to send data messages encrypted with its corresponding sender specific key (SSK). All members use the shared group data key to encrypt and decrypt data messages sent by members, and use the SSK to decrypt data messages sent by an associated non-member user. The protocol is claimed to achieve scalability and prevent several active and passive attacks, including unauthorised joining the routing multicast tree.

5 Group communication-oriented networks

This section reviews some SGC frameworks which have been implemented on several existing networks, including multi-agent systems (MASs), personal area networks (PANs) and IP multicast networks.

5.1 Multi-agent system

An MAS fundamentally consists of three components: agents, hosts and controller/coordinators. An agent can be a software code that runs on a host, operates in an autonomous manner, interacts with other agents and connects to one or multiple agent coordinators. An MAS is agent-based, implying that security services must be provided to end-to-end communications at the agent level, not at the host level. Keys and other group-related resource and information are usually stored in agents and protected from hosts on which these agents operate.

Li and Lan [17] proposed a mobile agent system operating through a secure and high performance agent-based multicast network. The proposed solution adopts the concept of multicast by supporting communications between an agent coordinator and an agent on a host or communications among agents at the agent level. The security solution uses two keys: a group key and a secret key. The centralised agent coordinator generates a secret key that is then cryptographically separated into secret key shadows, each shared individually by an agent. The key management is based on the concept of (k, n) threshold secrecy, by which the secret is shared among n agents and, to reveal the secret, the shares must be obtained from at least k agents. The secret key shadows are used to derive the group key. The group key and secret key shadows are protected from the resided hosts. The coordinator can evict any agent and take charge of rekeying by excluding the secret key shadow of the evicted agent from the original secret key. The existing agents can correctly compute the new group key while the evicted agent cannot.

Pros: Key secrecies are provided. Security and performance analysis of the proposed solutions are shown. The scheme was claimed to have reduced communications and processing overheads without solid proofs.

Cons: The scheme requires a priori embedment of the secret key shadow in the agent, and the scheme makes a weak assumption that an agent is well protected via cryptographic means and that each agent is trusted.

5.2 Personal area network

PAN communication is enabled by either wired technologies (i.e. USB and Firewire), wireless technologies (i.e. Bluetooth, Infrared and Wi-Fi) or a combination of both. In PANs, devices can communicate to each other and form the network around the person. Data can be passed through from one device to others or conveyed to other networks. Data can be encrypted by using a group key that is shared by all devices. The number of nodes is generally not large and most devices are operated by one person. With such characteristics, the central authority can be most effective in key management, and membership changes may not be frequent.

Shin *et al.* [18] proposed a framework consisting of key exchanged protocols against a compromised insider device: leakage-resilient and forward-secure authenticated key exchanges 1 and 2 (LRFS-AKE1 and LRFS-AKE2). The proposed protocols require a centralised server, which exchanges two long-term secret elements with a user: one for authentication (called the verification data) and another for securing its pair-wise communication (called the symmetric key). The group key generation and distribution occur within three phases. In the first phase, following LRFS-AKE1, the server and a user verify themselves by using the verification data, that is, a combination of a random number and the user's password, along with the symmetric key and the list of devices. Subsequently, a

pair-wise session key is generated individually for each device. In the second phase, following LRFS-AKE2, each device performs a contributory group key generation in an orderly manner, assisted by the server but without user interaction. The session key is used to secure the distribution of its contributed key portion. In the third phase, the same group session key is generated independently by each user.

Pros: Threat models are discussed; proposed protocols are suitable for PANs.

Cons: No rekeying mechanism exists; group key secrecy is not fully guaranteed due to the same password being used by the same user; a symmetric key is assumed to be done offline; additional user password is required; a centralised server is ignorantly assumed as trusted; and no membership change protocol exists.

5.3 Multicast security in IP multicast networks

Since 2000, the IETF MSEC working group aims to standardise SGC protocols over Internets with at least three security objectives [19]: first, providing fundamental security services, such as GKM, access control, group authorisation, group policy management and user and message authentication; second, extending operability from centralised networks to distributed networks where multiple trusted entities are deployed throughout networks and third, defending against network-based attacks.

Chaddoud and Varadharajan [20] proposed a secure source-specific multicast (S-SSM) communications architecture that offers two security services: access control and data integrity for commercial content delivery. It operates by using the protocol independent multicast-SSM (PIM-SSM) routers which form the backbone of the network. The PIM-SSM router is the router that provides security, especially access control, and Internet group management protocol (IGMP) version 3-based routing for SSM traffic. S-SSM divides the whole service area into domains and has two layers of controls: the domain-wide level via local controllers and the network-wide level via a global controller. The global controller and content distribution server are connected directly to the PIM-SSM routers. The global controller manages data distribution, authorises user access, generates channel keys and authorises rekeying. To manage subscribers, the IGMP version 3 is deployed in some PIM-SSM routers, which are located outside the backbone and connect directly to subscribers. In the IGMPv3/PIM-SMM routers, the local controller functionality is added to authenticate new subscribers, to distribute a channel key to subscribers, and to periodically rekey the channel key as authorised by the group controller.

Pros: Computation overhead is roughly analysed based on the number of computing operations; GKM, access control, traffic confidentiality and integrity and authentication services are offered; and dynamic membership is supported.

Cons: There is insufficient information about communication and computation overheads, and security analysis to substantiate the claim that the proposed scheme is very inefficient; and some communications on the offline channel may be required.

6 Challenging factors in designing secure GCSs

As illustrated in Tables 1 and 2, there is no unique scheme or system that can achieve all security requirements. Here, we summarise various perspectives and attributes in designing a secure and high performance GCS.

6.1 Environment and system performance

From the perspective of group management, a central group controller (and, in some systems, a key server) in a centralised GCS can afford intensive computations and storage overhead but, in return, becomes a point of the attack which threatens to shutdown all group operations. The other upsides are that high security can be achieved effectively and quickly, and each group member sustains less workload. A decentralised GCS reduces the workload performed by each sub-group controller. The apparent downsides include an additional communication overhead caused by communications among sub-group controllers, and the single point of failure problem. A distributed scheme increases workloads for each member in terms of storage and computation overheads, although the system is more scalable and eliminates the need of the central authority. For either environment (centralised or distributed), the design should optimise the system performance measured in terms of overheads (communication, computation and storage) burdened on each group member, the key server and the controller of the system.

6.2 Efficiency of key management and distribution

The efficiency of several security services relies on the strength of the key management and the cryptographic strength of the keys. An efficient GKM scheme should mainly reduce the time complexity and the computational load of key generation, key distribution and rekeying. The scheme should be scalable as the group size increases. Many efficient GKMs generate keys based on a structure of a key tree and a hierarchy of keys, especially for centralised and decentralised environments. In a distributed environment, a contributory GKM scheme seems more suitable.

doi: 10.1049/iet-ifs.2009.0261

6.3 Early detection and prevention

The secure GCS should be operated with strong authentication and access control mechanisms by which a violation of resource utilisation and unauthorised activities, for example, a member impersonation and a message fabrication, can be detected early and prevented. A group signature signed on messages can also provide source authentication, message integrity and non-repudiation services to the receiver and verifier. Since communication, storage and processing overheads are the primary cost for these security services, a trade-off between overheads and the protection level should be properly optimised.

6.4 Increased concern over privacy

Privacy becomes a major concern for users participating in group communications where there are a large number of message recipients so that message confidentiality may not be fully guaranteed, and security enforcement may not be possible or adequate. In general, anonymity service substantially increases overheads and the complexity. Thus, it may not be suitable in a deployment on distributed environments where resources are scarce. Instead, partial anonymity can be utilised in such a way that, for a large group, only partial identification is required to prove a rightful communication while it still preserves member privacy.

6.5 Implementation of security services for different applications

From the perspective of group-oriented applications, security services should be offered and compatibly interacted for any applications to achieve a high security level. Thus, the system should be transparent to applications.

7 Conclusions

This article provides a better understanding on various security requirements and security services in many GCSs. We have presented Figs. 2 and 3 to identify fundamental attributes for evaluating mechanisms that provide one or more security services to GCSs as well as additional properties corresponding to those supported security services. Then, based on properties in Figs. 2 and 3, we have presented the comparisons of those outstanding secure GCSs, as depicted in Tables 1 and 2. These tables show that most existing GCSs have been proposed based on only one or two security services and will not be able to satisfy other security requirements. Furthermore, these tables show how these schemes can be categorised, with respect to the security services offered, and what characteristics and attributes should be compared. Having understood the evaluation attributes, readers and researchers can exploit any other GCSs' merits, missing attributes or, perhaps, weaknesses that should have been further examined. To exemplify the usage of our evaluation attributes, we have evaluated and presented the advantages and disadvantages of three group communications networks in Section 5. The results showed that some important issues were not properly addressed in these GCS networks, such as no rekeying mechanism in [18], no overheads analysis in [19], and weak assumptions in [20], that might make these networks vulnerable against attacks. We have summarised some challenges for designing SGCs, such as system-wide performance, efficiency of key management, privacy issue, implementation and trade-off between security and overheads.

8 References

[1] SAKARINDR P., ANSARI N.: 'Security services in group communications over wireless infrastructure, mobile ad-hoc, and wireless sensor network', *IEEE Wirel. Commun. Mag., Spec. Issue Security Wirel. Mobile Ad Hoc Sensor Netw.*, 2007, **14**, (5), pp. 8–20

[2] BANERJEE S., BHATTACHARJEE B.: 'Scalable secure group communication over IP multicast', *IEEE JSAC*, 2000, **22**, (8), pp. 1511–1527

[3] WONG C.K., GOUDA M., LAM S.S.: 'Secure group communications using key graphs', *IEEE/ACM Trans. Network.*, 2000, **8**, (1), pp. 16–30

[4] AMIR Y., KIM Y., ROTARU C.N., SCHULTZ J.L., STANTON J., TSUDIK G.: 'Secure group communication using robust contributory key agreement', *IEEE Trans. Parallel Distrib. Syst.*, 2004, **15**, (5), pp. 468–480

[5] SUN Y., LIU K.J.R.: 'Hierarchical group access control for secure multicast communications', *IEEE/ACM Trans. Netw.*, 2007, **15**, (6), pp. 1514–1526

[6] ZHANG Q., WANG Y.: 'A centralized key management scheme for hierarchical access control'. Proc. IEEE GLOBECOM 2004, Dallas, Texas, December 2004, pp. 2067–2071

[7] CHEN Z., HUANG J., HUANG D., JIANHONG Z., YUMIN W.: 'Provably secure and ID-based group signature scheme'. Proc. IEEE AINA 2004, Fukuoka, Japan, March 2004, pp. 384–387

[8] LEE N.-Y.: 'Threshold signature scheme with multiple signing policies', *Proc. IEE Comput. Digit. Tech.*, 2001, **148**, (2), pp. 95–99

[9] ATENIESE G., CAMENISCH J., JOYCE M., TSUDIK G.: 'A practical and provably secure coalition-resistant group signature scheme'. Proc. IEEE CRYPTO 2000, Santa Barbara, California, August 2000, pp. 255–270

[10] XIAO L., LIU Y., GU W., XUAN D., LIU X.: 'A design of overlay anonymous multicast protocol', *ACM J. Parallel Distrib.*

Comput., Spec. Issue Security Grid Distrib. Syst., 2006, **66**, (9), pp. 1205–1216

[11] SYVERSON P.F., GOLDSCHLAG D.M., REED M.G.: 'Anonymous connections and onion routing', *IEEE JSAC*, 1998, **16**, (4), pp. 44–53

[12] REITER M.K., RUBIN A.D.: 'Crowds: anonymity for web transactions', *ACM TISSEC 1998*, 1998, **1**, (1), pp. 66–92

[13] GROSCH C.: 'Framework for anonymity in IP-multicast environments'. Proc. IEEE GLOBECOM 2000, San Francisco, California, December 2000, pp. 365–369

[14] DOLEV S., OSTROVSKY R.: 'XOR-trees for efficient anonymous multicast and reception', *ACM TISSEC 2000*, 2000, **3**, (2), pp. 63–84

[15] SHIELDS C., GARCIA-LUNA ACEVES J.J.: 'KHIP: a scalable protocol for secure multicast routing'. Proc. ACM SIGCOMM 1999, Cambridge, Massachusetts, September 1999, pp. 53–64

[16] SHIM Y.-C.: 'A new approach for secure multicast routing in a large scale network'. Proc. ICICS 2001, Xian, China, November 2001, pp. 95–106

[17] LI T., LAM K.-Y.: 'A secure group solution for multi-agent EC system'. Proc. IPDPS 2001, San Francisco, CA, April 2001, pp. 1749–1756

[18] SHIN S., FATHI H., KOBARA K., IMAI H.: 'A secure group communication framework in private personal area networks (P-PANs)'. Proc. ICWMC 2007, Guadeloupe, French Caribbean, March 2007, pp. 59–67

[19] HARDJONO T., WEIS B.: 'The multicast group security architecture'. IETF working group, multicast security (MSEC) chapter, retrieved from http://www.ietf.org/html.charters/msec-charter.html and http://www.ietf.org/rfc/rfc3740.txt, accessed December 2009

[20] CHADDOUD G., VARADHARAJAN V.: 'Efficient secure group management for SSM'. Proc. IEEE ICC 2004, Paris, France, June 2004, pp. 1436–1440

doi: 10.1049/iet-ifs.2009.0261