Security Architecture for Satellite Services over Cryptographically Heterogeneous Networks

Yingli Sheng[1], Haitham S. Cruickshank[1], Martin Moseley[2], and John Ashworth[2]

[1] Centre for Communication Systems Research
University of Surrey
Guildford, United Kingdom
{Yingli.Sheng,H.Cruickshank}@surrey.ac.uk
[2] EADS Astrium
Portsmouth, United Kingdom
{Martin.Moseley,John.Ashworth}@astrium.eads.net

Abstract. The rapid growth in the demand for Internet services and many new applications has driven the development of satellite, which are the preferred delivery mechanism due to its wide area coverage, multicasting capacity and speed to deliver affordable future services. However, security has been one of the barriers for satellite services, especially for domains spanning over cryptographically heterogeneous networks. In this paper, a scalable and adaptable security architecture is specified to protect satellite services. Two major issues in the proposed security architecture, key management and policy provisioning, are presented and analyzed. And three scenarios, mobile network, fixed network and Delay Tolerant Network (DTN), are presented, with details on characteristics and security features.

Keywords: satellite, Heterogeneous network, policy, key management, mobile network, Delay Tolerant Network.

1 Introduction

Satellites will be an integral part of the Internet and next generation access technologies such as wireless, mobile and terrestrial broadband. As such, the broadcast nature of satellite coverage can be exploited, costs can be shared among large group of terminals providing a low-cost wide-area Internet multicast service. In addition, group-oriented applications are increasingly deployed over the Internet such as video conferencing, video on demand (VoD), TV over Internet and broadcasting stock quotes. A difficult barrier that prevents the wide exploitation of satellites and the group-oriented applications is the security provisioning for a large and cryptographically heterogeneous multicast group that span multiple domains.

It is proposed in the paper a scalable and adaptable security architecture that protects multicast data according to the cryptographic requirements of a variety of cryptographic domains. This work defines a new satellite multicast security architecture that addresses the specific obstacle that currently impedes development of large scale multicast security services that spans several cryptographically heterogeneous domains. By

R. Dhaou et al. (Eds.): PSATS 2013, LNICST 123, pp. 102–114, 2013.

introducing scalable key management and security policy mechanism, some of the security barriers that inhibit the integration of satellite networks with other network such as next generation mobile networks, would be removed. The major research issues in the security architecture are presented and analyzed, namely key management and security policy provisioning. Also, three sample scenarios are presented, including characteristics and security requirements for each of them.

2 Objectives

Future Internet will be a conglomerate of heterogeneous networks and systems such as satellite, next generation mobile, mobile adhoc and sensors nodes. It is envisaged that satellites will be part of broadband, mobile and Delay Tolerant Networking (DTN) service scenarios, which can span multiple security domains that are cryptographically heterogeneous. The concept of domains is used widely in the Internet. It is also applicable to group-key management to effect scalability, where members are divided (logically or physically) into domains or subgroups. In summary, at least two general types of domains are possible for secure group management:

- Domains according to data encryption: Here, the domains demarcate regions within which differing Traffic Encryption Key (TEK) are used to encrypt the group data.
- Domains according to key management: Here, the domains demarcate key management regions, where each region is associated with a different set of Key Encryption Keys (KEK) for the purpose of managing and disseminating the TEK, which is a common group data key.

Securing such service scenarios could be very challenging due to trust issues, key distribution, policy dissemination/management and multiple encryption/decryption across these domains.

The objective of the work is to specify a scalable and adaptable security architecture that is hierarchical and distributed, in order to protect unicast, multicast and broadcast data for a variety of cryptographically heterogeneous networks. The security architecture involves scalable key management and policy management entities. Such architecture should fit all the three scenarios mentioned above: mobile broadband, fixed network terminal and DTN.

3 System Architecture

It is presented in this section an innovative architecture for securing multicast services across heterogeneous security domains.

The architecture for securing multicast services across heterogeneous security domains is shown in Figure1. There are three novel concepts in this architecture:

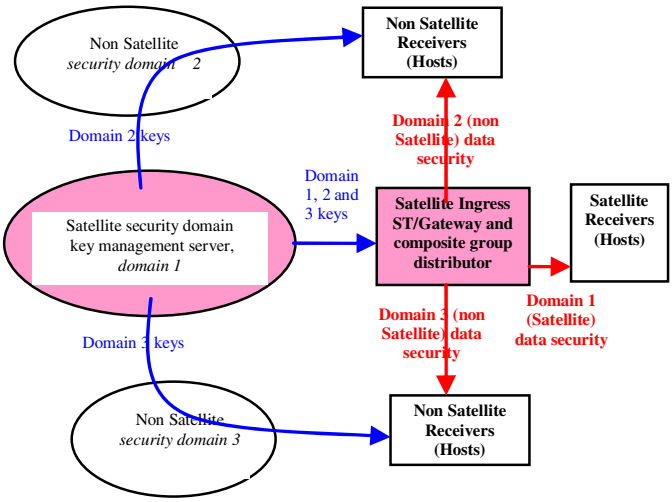

Fig. 1. Secure multicast service across heterogeneous security domains

- The first concept is the adaptive and scalable group key management. It will use adaptive grouping of members into encryption domains (subgroup) that use the same TEK. The partitioning will be made in a way that reduces both re-keying using KEKs and key translation overheads within the overall heterogeneous group. This concept promotes adaptability to changing membership dynamics in various domains.
- The second concept is the use of Data Distributors that disseminate the encrypted data with different keys for each domain. This will eliminate the need for encryption/decryption at security gateways at the ingress of each domain.
- The third concept is the use of security policies, especially for the distributed architecture to delegate trust and role to various entities in each domain. This will promote scalability and adaptability to changing security and threats situations. As such, policies can govern key dissemination, access control, re-keying of group-shared keys, and for the actions taken when certain keys are compromised.

The solution complements the existing link layer security solutions in satellite, digital video broadcasting (DVB), UMTS and WiMAX networks. However, it requires that data security should be implemented in a layer in the protocol stack that is common to all domains (e.g. satellite, UMTS and WiMAX), such as:

- IP network layer security (using IPSec);
- Transport layer security (TLS);
- Any application layer security.

4 Major Research Issues

There are several obstacles against the widespread deployment of multicasting services [1][2]. One of them is security. The security mechanisms for unicast are not adequate for the multicast scenario since multicast security mechanisms have scalability and efficiency constraints [3][4][5]. The work proposed in this paper aims to address gaps in secure multicast such as IP Multicast group key management and policies, with a particular focus on a group that spans many domains including a satellite network. Thus, there are two major research issues:

- Multicast key management in cryptographically heterogeneous domains
- IP multicast security policy provisioning

A Key Management

In a simple case, symmetric cryptography is used by the sender/source and the receivers/destinations, where the data is encrypted by the sender and decrypted by the receivers. The shared key is commonly referred to as the group-key or TEK, since only members of the multicast group are in possession of the key. The use of cryptography necessitates the delivery or dissemination of group keys. Group-oriented security, and more specifically the key management, has been researched for more than two decades. Most of the earlier work has focused on cryptographic approaches to manage keys for hierarchical organizations [6][7][8]. And satellite networks had their research on large scale secure multicast [9][10][11].

Rekeying in secure multicast is needed to preserve forward and backward secrecy whenever members join or leave. Thus rekeying overheads increases as the multicast group gets bigger. The concept of domains is also applicable to group-key management to effect scalability, where members can be divided (logically or physically) into domains (subgroups) [3][12]. However, a clash exists between re-keying overhead and computation overhead for key translation. Finding a trade-off between these two conflicting overheads is essential in the case of networks with resource constrained devices, such as sensors and Mobile Ad hoc NETworks (MANETs) and in the case of very large groups such as satellite multicast. At least two general types of domains are possible for secure multicast management:

- Domains according to data encryption: Here, the domains demarcate regions within which differing group-keys (data keys) are used to encrypt the multicast data. Thus, each domain is associated with a unique group-key, and "crypto-translations" (decryption using one key, followed by encryption using another key) must be carried out at the domain boundaries. Group-members residing within each domain would be in possession of a unique group-key (per domain).
- Domains according to key management: Here, the domains demarcate key management regions, where each region is associated with a different set of key management keys (KM-keys) for the purpose of disseminating the common group-key (TEK). Thus, each domain would manage its own km-keys (e.g., different rekey period for KM-keys), even though these are used to create safe passage for the common (group-wide) TEK from a key-source,

such as a key server, to each of the receivers residing in differing key management domains.

There exist a clash between re-keying overhead, and computation overhead: on one hand, using a single encryption domain increases the re-keying overhead and hence does not scale to large and highly dynamic groups, while it saves computation power which would have been spent in key translation. On the other hand, partitioning the group into different encryption areas reduces the re-keying overhead, but introduces additional computation overhead and delivery delays because of the requirement of key translation. The scalable key management scheme aims to find a good trade-off between these two conflicting overheads.

B Security Policy

Security policies provisioning is another focal point of the proposed architecture. Similar to other aspects of networking, the correct definition, implementation and maintenance of policies governing the various aspects of multicast security are important factors. Those which are directly related to multicast security include the policies for key dissemination, access control, re-keying of group-shared keys, and for the actions taken when certain keys are compromised [13]. The trust model is a critical issue for secure group communications, which can be established and managed using rule-based security policies. For large scale groups that span several security domains, security management might be delegated to group controllers (key managers) in each domain. Delegation of trust using policies allows the efficient working of distributed security management architecture [14][15]. Thus the use of such policies will help the security integration of satellite network with other networks. Through policies, a system may address the needs of all group participants in real time. The security policy could address the following requirements [16]:

- Identification - Each participant and group can be unambiguously identified.
- Authorization - A group policy can identify the entities allowed to perform protected actions. Group authorization partially determines the trust embodied by the group.
- Access control - Allowable access to group action can be stated by policy.
- Mechanism - Each policy can state how the security requirements of the group are to be addressed.
- Verification - Each policy can present evidence of its validity such as proof of its origin and integrity.

A Reference Framework has been defined and standardized and it addresses all problem areas mentioned above [12][17]. The framework presents a set of functional building blocks that should be tackled for any secure multicast architecture design. It also expresses the complex multicast security from the perspective of architecture (centralized/distributed), multicast group types (1-to-*N* and *M*-to-*N*), and classes of protocols (the exchanged messages) needed to secure multicast packets.

However, currently very little work exists on using security policies for distributed key management, particularly for satellite networks. As such, security policies should

be used to delegate trust to key managers and data distributors in various domains. If the multicast group membership is highly dynamic, then policies will also enable adaptive formation and deletion of data encryption domains depending on the subgroup membership dynamics. Security policies are used in the proposed architecture to promote scalability and adaptability in large heterogeneous multicast groups.

5 Scenarios

In this section, three scenarios are defined: mobile network scenario for the applications such as mobile broadband, fix network scenario for the applications such as SMART METER, broadband access and Delay Tolerant Network (DTN) scenario for the space applications such as Deep Space. The scenarios are described and the features are discussed in this section.

A Mobile Scenario

One typical application of mobile scenario is mobile broadband service, which includes web browsing and possibly video streams. Security, as one of the important features of mobile broadband, must be provided to essential signalling messages, but might not necessarily to the large amount of packet data.

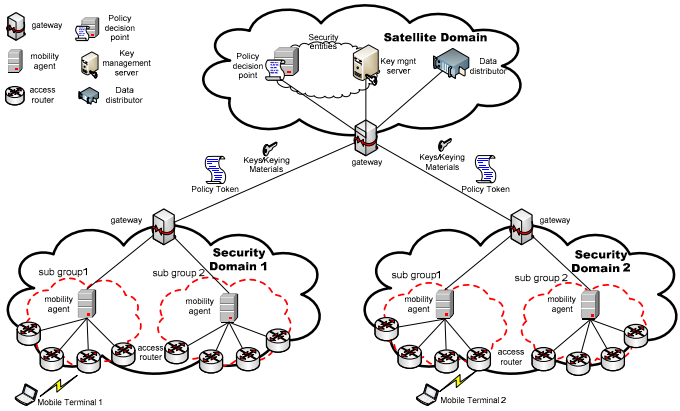

Fig. 2. Mobile scenario

As shown in Figure 2, three domains are involved in the mobile scenario: satellite domain, security domain 1 & 2. Security domain 1 &2 are assumed to be cryptographically separated. It is possible that different encryption/decryption algorithm, different key size are used to secure the signalling/traffic data in security domain 1 & 2. The satellite domain provides the ability for centralized key management and policy generation.

1) Satellite domain

a) Data distributor
Disseminate the encrypted data with different data keys for each domain. This entity eliminates the need for encryption/decryption at security gateways at the ingress of each domain.

b) Key management server
Dynamically generate different set of key management keys for different regions. The adaptive and scalable group key management is enabled by the use of key server. It uses adaptive grouping of member into encryption domains that use the same data key, therefore, it reduces re-keying and key translation overheads.

c) Policy decision point (PDP)
It acts as policy server which generates policy (such as policy token [18]) to delegate trust and defines different security mechanisms to various domains. Policy enables adaptable security solutions for changing security and threats situations. Therefore, the resilience to changing security environment is improved. Generally, policy can define key/keying materials dissemination, access control, re-keying conditions, actions taken when a key is compromised, and etc.

It should be noted that the centralized scenario is illustrated in Figure 2. In a centralised scenario, the policy decision point and key server are located in the satellite domain, and relevant security information is disseminated to various security domains. The policy enforcement point (PEP), which cooperates with PDP to enforce policy to the end terminals, can be collocated with entity in each security domain, such as the mobility agent. The PEP can issue policy request on behalf of the end user and handle policy response from the PDP. If distributed system is required, the PDP/key server should be available in each of the security domains, providing the ability to generate policy and set of keys locally within the particular security domain. And the local PDP/key server should be able to operate in a cooperative manner to achieve optimized performance.

2) Security domain1 & 2
In both of security domain 1& 2, the following entities are involved:

a) Gateway

It is the point of entry or exist for the security domain, providing connectivity to the satellite domain.

b) Mobility agent

It provides mobility management service to the mobile terminals, including location updates, forwarding traffic data, and etc.

c) Access router

It is a layer-3 router, providing network access to the mobile terminal. The access routers can be managed by the mobility agent.

d) Mobile terminal

It is the mobile user, who would like to use the network resources. It can perform micro-mobility handover within one mobility agent subgroup and can also perform macro-mobility handover across mobility agents/networks.

3) Characteristics

Some characteristics of mobile scenario are:

a) Moderate bandwidth availability
b) Limited number of security domains
c) Limited coverage areas

4) Security features

Some security features of mobile scenario are:

a) Specific key management requirements: multiple encryption/decryption domains are needed

b) Moderate data key updates due to moderate data rate in the forward link

c) For multicast services, moderate/fast changing group membership due to the nature of mobile services

d) Either centralized or distributed key/policy management architecture can be considered.

e) For the delay sensitive data in mobile applications, it is required to reduce the negative impact of security on delays by integrating security design with mobility protocols.

f) Due to the nature of valuable bandwidth resources, minimizing signalling overhead introduced by security mechanism is essential. The tradeoffs between strong security design which desired by the cryptography fans and the overhead introduced by security need to be considered.

B. Fixed Network Scenario

The fixed network scenario can be applied to broadband access in rural area, where DSL lines are not applicable, or specific application such as SMART METER/GRID.

As shown in Figure 3, three domains are involved in the fixed network scenario: satellite domain, security domain 1 & 2. Security domain 1 &2 are assumed to be cryptographically separated. The satellite domain remains the same as in the mobile scenario. While in each of security domain, instead of roaming mobile terminals, there are fixed terminals. The terminals can be broadband service terminals, or other devices, such as SMART METER device installed in the end users' home/office. All of the terminals are connected to the aggregation router, which provides the ability of

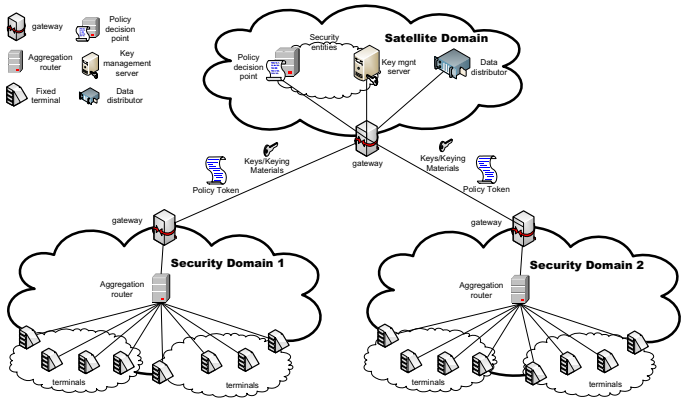

Fig. 3. Fixed network scenario

data aggregation. And the aggregation router is connected to the external network, via gateway. The fixed terminals (for a broadband service) can be connected directly to the aggregation router for the broadband service, and the aggregation router then connects to the satellite access gateway. If the SMART METER application is considered, the terminals are SMART METER devices installed at the end user's home/office to collect the electricity/gas/water meter information. Of all Smart Meter technologies, one critical technical problem is communication. Each meter, especially the sensitive user ID or billing related information, must be reliably and securely transferred to the central location. Considering the varying environments and locations where meters are found, that problem can be daunting. The existing solutions proposed are: the use of cell/pager networks, satellite, licensed radio, combination licensed and unlicensed radio, power line communication (PLC). Not only the medium used for communication purposes but the type of network used is also critical. Fixed wireless, mesh network or a combination of the two have been deployed for SMART METER application. There are several other potential network configurations possible, including the use of Wi-Fi and other internet related networks. No one solution seems to be optimal for all applications. Rural utilities have very different communication requirements from urban utilities or utilities located in difficult locations such as mountainous regions or areas ill-served by wireless and internet companies. Thus, providing SMART METER service using satellite is ideal for rural or difficult locations, and it is also possible to application in urban areas as well. There is a growing trend towards the use of TCP/IP technology as a common communication platform for Smart Meter applications, so that utilities can deploy multiple communication systems, while using IP technology as a common management platform.

1) Characteristics

Some characteristics of fixed network scenario are:

a) Higher bandwidth availability for forward link and limited bandwidth in the return link

b) Multiple security domains
c) Wider coverage area comparing to mobile scenario

2) Security features
Some security features of fixed network scenario are:

a) multiple encryption regions due to the multiple administrative domains
b) moderate/frequent data key updates might be necessary due to higher data rate in the forward link
c) For multicast services, slow/static group membership due to the nature of fixed network terminals
d) Centralised key/policy management architecture is the preferred solution.
e) Access control is one of the major concerns of SMART METER application. It is to ensure only devices authorised by the customer and energy supplier are allowed to interact with metering system.
f) How to manage and use the data key is essential. For the broadband services, the main types of communication that are supported by fixed network are voice, data transfer, video/images and web browsing. It might not be necessary to use data key to secure all of the traffic (such as large volumes of multimedia traffic). How to define the security level of different traffic becomes a challenge. For the SMART METER application, each meter, especially the sensitive user ID and billing related information, must be reliably and securely transferred to the central location.

C. DTN Scenario: Deep Space

Space exploration started in early sixties and since then the interest towards deep-space communication continuously increased especially from the scientific point view, thus paving the way for the Moon human exploration and then the Mars missions. More recently, the current advances and trends in technology have pushed the space agencies to a new and more futuristic concept of space exploration: the Solar System Internet. In fact, it consists in the deployment of a real Internet over the space, able to connect Earth centers to remote sites, located in possibly different places of the Solar System, such as Mars, Saturn, and Mercury. Consequently, it is immediate to think of a complex deep-space network (Figure 4), where data transaction and routing operations are performed seamlessly and autonomically, thus reducing the manual intervention to the least. The human assistance would be still needed to provide recovery to emergency situations that the implemented fault resilience model could not handle. Besides the attracting perspective, this future scenario may offer benefits in terms of scientific studies and possible revenues for the aerospace industries.

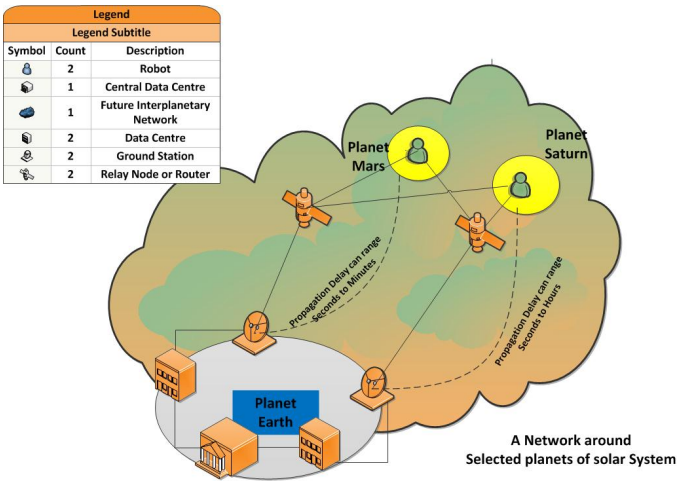

Fig. 4. DTN scenario: A Diagram showing a future network along planets of solar systems

1) Characteristics

Some characteristics of DTN scenario are:

a) Extremely limited bandwidth availability

b) Limited number of security domains.

c) Frequent disconnection/disruptions

d) Very large propagation delays. Depending on the specific addressed space mission, the propagation delay can range from a few seconds (e.g., Earth-Moon) to several minutes (e.g., Earth-Mars), to even hours (e.g., Earth-Saturn, Earth-Pluto).

e) Scarce and highly asymmetric link data rate. Because of the reduced spacecrafts' size, the deployed antenna can be only of reduced dimensions, thus implying small data rate available. In addition, most of part of data traffic flows though the downlink (e.g., measurement, image transfer), whereas the uplink is principally used for transmitting telecommand messages. As a result, strong asymmetry between data rates available on downlink and uplink respectively is experienced, being as high as 10000 to 1.

f) Limited storage availability. The limited dimensions of the space crafts pose additional constraints on the on-board storage, which plays some role for routing and buffering.

g) Degraded link quality. The long distances determine high free-space-loss to which also weather fading may add, occurring in case of Ka band transmission. Besides, in case of optical laser technology, additional quality impairments may take place, resulting in non negligible BER or PER.

h) Intermittent visibility between Earth and other remote planets, because of the relative movement around the Sun, resulting in tight transmission schedule to take advantage of the available resources. Finally, this leads to an overall reduced throughput measure, if compared to the total mission time. However, by using the

relay nodes or routers in the space, increased data rate and more communication opportunities can be achieved by using DTN store and forward mechanism

2) Security features
Some security features of DTN scenario are:

a) Limited number of encryption regions, due to the nature of space application
b) Slow data key updates
c) For multicast services, slow changing/static group membership
d) Distributed key/policy management architecture is the preferred solution, due to the sparse nature of space communications..

6 Conclusion

While the advantages of multicasting services over satellite networks are clear, security as one of the obstacles poses great challenges in terms of scalable key management and adaptable policy provisioning. An innovative security architecture is proposed in this paper to address the security challenges, with a particular focus on key management and security policy. The major issues on multicast key management/security policy are discussed. A brief literature review is provided and existing problems are highlighted. Also, three scenarios are defined for future implementation: mobile network scenario for the application such as mobile broadband, fixed network scenario for the application such as SMART METER/GRID and DTN scenario for the application of Deep Space. The characteristic of each scenario is analyzed and security requirements are also drawn.

Based on the security architecture, protocols between key managers, policy server and data distributor need to be defined in the future. Group Secure Association Key Management Protocol (GSAKMP) in [14] provides secure communications between group owner, key mangers, senders and receivers. Either GSAKMP-type protocol will be used to establish secure communications between data distributors the other entities or a new protocol will be developed, depending on the architecture requirements. If a new protocol is required, the proposed protocol will be analyzed and verified by model-checking or theorem-proving techniques.

References

[1] Brown, I., Crowcroft, J., et al.: Internet Multicast Tomorrow. Internet Protocol Journal 5(4) (2002)
[2] Diot, C., Levine, B.N., Layers, B., et al.: Deployment Issues for the IP Multicast Service and Architecture. IEEE Network 14, 10–20 (2000)
[3] Challal, Y., et al.: Adaptive clustering for Scalable Key Management in Dynamic Group Communications. International Journal of Security and Networks (2007) ISSN 1747-8413

[4] Rafaeli, S., Hutchison, D.: A Survey of Key Management for Secure Group Communication. ACM Computing Surveys 35(3), 309–329 (2003)
[5] Wittmann, R., Zitterbart, M.: Multicast communication: Protocols and applications. Morgan Kaufmann (2001) ISBN 1-55860-645-9
[6] Koyama, K., Ohta, K.: Identity based conference key distribution systems. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 175–184. Springer, Heidelberg (1988)
[7] Ballardie, A.: Scalable Multicast Key Distribution. RFC 1949, IETF (1996)
[8] Steiner, M., et al.: Diffie-Hellman key distribution extended to group communications. In: Proceedings of the 3rd ACM Conference on Computer and Communications Security. ACM (March 1996)
[9] Cruickshank, H., et al.: Securing multicast in DVB-RCS satellite systems. IEEE Wireless Communications, Special Issue on Key Technologies and Applications (October 2005)
[10] Ng, D., Cruickshank, H., Sun, Z., Howarth, M.P.: Dynamic Balanced Key Tree Management for Secure Multicast Communications. IEEE Transactions on Computers (2007)
[11] Zhang, Y.: A multilayer IP security protocol for TCP performance enhancement in wireless networks. IEEE Journal on Selected Areas in Cmmunications 22(4) (May 2004)
[12] Hardjono, T., et al.: The Multicast Group Security Architecture. RFC 3740 (2004)
[13] Harney, H., Harder, E.: Multicast Security Management Protocol (MSMP) Requirements and Policy. IETF, draft-harney-sparta-msmp-sec-00.txt (March 1999)
[14] Harney, H., et al.: GSAKMP: Group Secure Association Key Management Protocol. RFC 4535 (2006)
[15] Christian, T., Riguidel, M.: Distributed trust infrastructure and trust-security articulation: Application to heterogeneous networks. In: IEEE, Proceedings –20th International Conference on Advanced Information Networking and Applications, pp. 33–38 (2006)
[16] Harney, H., et al.: Principles of Policy in Secure Groups. In: Proceedings of Network and Distributed Systems Security 2001. Internet Society (2001)
[17] Baugher, M., et al.: Multicast Security Group Key Management Architecture. RFC 4046 (2005)
[18] Colegrove, A., Harney, H.: Group Security Policy Token v1, RFC 4534, IETF (June 2006)