NAMEPS: N -Tier Satellite Multicast Security Protocol Based on Signcryption Schemes

Attila Altay Yavuz
Computer Engineering Department
Bogazici University, Istanbul, Turkey.
Email: attila.yavuz@boun.edu.tr

Fatih Alagz
Computer Engineering Department
Bogazici University, Istanbul, Turkey.
Email: alagoz@boun.edu.tr

Emin Anarim
Electrical Engineering Department
Bogazici University, Istanbul, Turkey.
Email: anarim@boun.edu.tr

Abstract— **In this paper, we propose a new N-tier sAtellite Multicast sEcurity Protocol based on multi-recipient Signcryption schemes (NAMEPS). Our protocol is especially designed for very large and highly dynamic satellite multicast systems which require high security and reliability. Our N-tier architecture significantly reduces workload of the satellite layers especially for bandwidth consumption, computation resources and storage requirements. N-tier approach localizes effects of the rekeying operation (forward-backward security) and provides significant performance gain. Moreover, batch keying and ticketing mechanisms are used which additionally reduce workload of the satellite and terrestrial layers. Also, as a novel approach for cryptographic method, our protocol uses multi-recipient signcryption scheme, which provides confidentiality, authentication, unforgeability and non-repudiation together, more efficiently than classical sign-then-encrypt approaches. As a result, NAMEPS has many advantages for very large, dynamic and security critic satellite multicast systems.**

I. Introduction

Secure satellite multicast systems (SSMS) have critical importance in today's communication systems. Many real time applications such as military command and control, secure audio-visual data multicast, pay TV and file distribution applications need secure, reliable and high performance satellite multicast systems. However, providing security and effectively managing cryptographic keys in SSMS are challenging problems. Problems become much severe especially for SSMS, which have very large number of members and dynamic member join-leave characteristics.

Satellite multicast systems are more vulnerable to security attacks. Eavesdropping and active intrusion are much easier than terrestrial fixed networks. Also, SSMS are resource limited especially for power and bandwidth consumptions. One of the most important issue is that, in order to provide forward and backward security, whenever a member join-leave event occurs, group key must be updated (rekeying). Rekeying causes massive workload and significant performance problems especially for very large and dynamic SSMS.

In this paper, to address aforementioned problems, we propose a new **N**-tier s**a**tellite **m**ulticast s**e**curity **p**rotocol based on multi-recipient **s**igncryption schemes (NAMEPS). NAMEPS is especially designed for very large (10^6 member or more) and highly dynamic (includes many mobile unit) SSMS which require security and high performance together.

NAMEPS uses N independent key distribution layers to handle very large satellite multicast systems. NAMEPS especially addresses rekeying workload over satellite layers, which is the major source of the performance problem. In NAMEPS, using N-tier architecture, whenever a member join-leave event occurs, rekeying is realized on only related layers and other parts of the system are not affected from modifications. This approach provides significant performance gain for satellite layers as well as terrestrial layers. Note that, most resource limited component of the SSMS is satellite layers and NAMEPS especially reduces workload of the satellite layers. Also, hierarchical structure of NAMEPS is compatible for military applications as well as commercial applications. NAMEPS uses ticketing and batch keying mechanisms which also reduce workload of the satellite and terrestrial layers. NAMEPS consists of GEO, MEO and LEO satellite layers as satellite layer and Terrestrial Units (TU), Major Mobile Units (MMU) and members layer as terrestrial layers.

In SSMS, apart from architecture, cryptographic primitives have critical importance for security and performance aspects. Cryptographic primitives must provide major cryptographic goals such as confidentiality, authentication, integrity, unforgeability and non-repudiation. Moreover, in multi-tiered architectures and especially for satellite networks, cryptographic workload may cause non-neglible delay and power consumption problems. In NAMEPS, to address these problems, as a novel approach, multi-recipient signcryption (SCS1M) methods are used for cryptographic key management. Signcryption is a relatively new concept, providing confidentiality, authentication, integrity, unforgeability and non-repudiation together more efficiently than classical sign-then-encrypt approaches. Using SCS1M in SSMS provides significant advantages for both cryptographic workload and especially bandwidth consumption. As far as our concern, multi-recipient signcryption schemes have not been used in SSMS before.

II. Related Work

Many different key management protocols have been proposed to solve aforementioned problems. Generally, we can analyze group key management protocols such as centralized and decentralized approaches [1], [2], [3].

In centralized group key management protocols, there is only one central entity that controls whole group. No auxiliary

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

entity (TTPs or additional KDCs) is required to perform key distribution. However, single point of failure problems may arise. In these approaches, hierarchical methods, which can scale group size logarithmically, are used. LKH [4], OFT [5], [6] and ELK [7] are well-known protocols using these approaches. In decentralized group key management protocols, large group is split into small sub-groups. Different controllers are used for each sub-group. Iolus [8] and Kronos [9] are based on this approach. Hybrid protocols integrating these two approaches can be found in [10], [11], [12]. Note that, [11] and [12] are especially designed for SSMS. In [11], two layered architecture, TTPVSS (Two-tier Pintsov Vanstone Signature Scheme), has been proposed, using LKH protocol in each of its layers. TTPVSS applies independency of layers principle to SSMS. With this way, effect of the modifications, which are performed over single point of the SSMS, are restricted in a local region and other parts of the SSMS and especially satellite is not affected from modifications. This provides significant performance gain for satellite. Also, as a novel approach, TTPVSS uses ECPVSS (Elliptic Curve PVSS) which provides many advantages. Study in [12] extends principles of TTPVSS to three-tiered architecture and utilizes some properties of satellite layer. Also, as a novel approach, it uses ECMQV (EC Menezes-Qu-Vanstone) and STAKE (Signcryption Type Authentic Key Establishment Scheme) cryptographic primitives in SSMS.

III. Major Cryptographic Methods Used in NAMEPS

In NAMEPS, as a novelty, we use signcryption based cryptographic primitives. Signcryption is a relatively new concept in cryptography. Signcryption scheme is a cryptographic method that fulfills both the functions of secure encryption and digital signature, but with a cost smaller than that required by sign-then-encrypt approach [13], [14]. Many efficient signcryption schemes have been proposed. Shortened El-Gamal signature based signcryption is one of the most characteristic signcryption scheme [14], [15]. It uses El-Gamal variants and shorted signatures such as SDSS1-2(Shortened Digital Signature Standard 1 and 2) to create digital signcryption schemes. Also, extension of signcryption schemes to ECDLP (EC Discrete Logarithm Problem) is given in [16] . Thus, methods that are used in NAMEPS can be easily extended to the EC domain. Signcryption schemes are used to create key agreement schemes [17]. Many implementations of signcryption schemes for network protocols exist [18].

We do not give detailed steps of the signcryption scheme that we use in NAMEPS. We preferred SCS1M (Signcryption Scheme for Multiple Recipients) in [15], that is based on SDSS1. However, we give general notations that are used in NAMEPS for signcryption based scheme. Note that, public-private key generation and other rules are given in section IV.

p :Large prime number, q :A large prime factor for $(p-1)$, g :Generator of the group with order q modulo p, H :Unkeyed cryptographic hash function, H_K :Keyed cryptographic hash function, $(E-D)_K$:Symmetric encryption-decryption function with private key K, (c,z,s) $triplet$: c includes message ciphertext, z includes keyed hash value of message, s is used for recovery purpose together with z and required public-private keys of the parties of the communication, $BBS(Blum-Blum-Shub)$:Cryptographically strong pseudo random number generator [3]. In our notations, BBS takes two types of parameters. First type of parameter determines upper or lower bound for number of elements that BBS generates. Second type of parameter is a seed value which triggers BBS for random number generation. $SPNG$: Strong prime number generator, $Generator$:Generates a generator g for related field, n :Number of members in SSMS, n_s :Number of satellites in satellite layers, l :Number of TU in SSMS, n_m :Number of MMU in SSMS, M : Bulk multicast data. Other notations are given when they are needed.

In NAMEPS, for bulk data transmission, symmetric key cryptography primitives are used. Block ciphers and stream ciphers can be used for these purposes [19].

IV. Details of NAMEPS

A. Properties of NAMEPS

Our protocol uses N-tier architecture to manage very large and dynamic satellite multicast groups. We use independency principle of [11] in our N-tier architecture providing novel approaches for design and cryptographic method aspects. The major idea behind of NAMEPS is that, providing independency between layers reduces rekeying workload of the satellite significantly. However, N-tier approach requires multiple encryptions between layers which cause performance deteriorations. To address these problems, NAMEPS offers appropriate cryptographic methods that make N-tier approach feasible and secure.

Using independency principle, whenever a member join-leave event occurs, effects of the modifications are restricted on their related areas and remainder parts of the system are not affected from modifications. However, unlike [11], NAMEPS uses ELK protocol in each of its layer. ELK protocol has advantages for rekeying cost and size of packets when compared with LKH protocol. Also, validation tickets are used which provide advantages for reliability. As mentioned in section III, our protocol uses signcryption based cryptographic method SCS1M to transmit these keys securely. These improvements significantly reduce rekeying workload and number of keys which are stored on the satellite layer. Note that, satellite layers are the most resource limited components of the multicast system. Thus, it is critical to reduce the workload of these components.

Mainly, NAMEPS consists of three satellite layers and three terrestrial layers. Responsibilities and properties of each layer are given below.

B. Detailed Description of NAMEPS

1) Initialization, Key Distribution and Data Multicast in GEO Satellite Layer: In NAMEPS, top level of the hierarchy is GEO satellite. GEO satellite is responsible for generating all group keys and group key seeds for lower layers. Also,

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

GEO satellite actively involves bulk data multicast for regions that LEO and MEO satellites can not cover.

GEO satellite uses group key to distribute seeds and other group keys using SCS1M. GEO satellite determines group keys which LEO and MEO satellites use to securely communicate with TUs and MMUs. To do this, GEO satellite generates group key seeds st_i where $1 \leq i \leq n_s$. Each LEO and MEO satellite is assigned to a group key seed st_i. LEO and MEO satellites generate group keys $t_{i,j}$ using group key vector seed st_i where $j \geq l + n_m$. In here, $t_{i,j}$ denotes j'th group key that is used by i'th satellite in LEO and MEO satellite layers. Major purpose of seeds values (vector st) is to provide batch keying. Using batch keying, instead of transmitting group keys one-by-one, only their seed values are transmitted, which provides significant bandwidth advantages. Also, group key seeds for MMUs , sm_i where $1 \leq i \leq n_m$, are generated with same method and aim by GEO satellite. Note that, this approach is also effectively used in [12]. In NAMEPS, additionally, validation tickets are used which provides important flexibility. Moreover, as a cryptographic method, SCS1M is used in each layer that provides additional advantages for batch keying, cryptographic workload and bandwidth consumption. However, in [12], cryptographic methods are different for each layer such as ECPVSS, IMC (Improved Merkle Cryptosystem), ECMQV and STAKE.

GEO satellite performs following steps:

1.1 Key generations: $p = SPNG(\geq\ 1024\ bits), g = Generator(p)$,

$(GK, x_a, y_a, st_i, sm_i, v_i) = BBS(=1, =1, =1, \geq n_s\ , \geq n_m, = n_s)$ and $y_i \leftarrow$(obtained from each LEO-MEO satellite) where $1 \leq i \leq n_s$. Here, v_i are random numbers, x_a is private and y_a is public key of GEO satellite.

1.2 GEO satellite signcrypts necessary keys and data for the lower layers. Data packet M includes group key seeds st_i, sm_i and multicast data for GEO satellite m_{geo}.

$M = (st_i, sm_i, m_{geo})$, $h = H_{GK}(M)$, $c = E_{GK}(M, h)$,

$k_i = H(y_i^{v_i} \bmod p)$, $k_i \rightarrow (k_{i,1}, k_{i,2})$, $c_i = E_{k_{i,1}}(GK)$,

$z_i = H_{k_{i,2}}(M, h)$, $s_i = v_i(z_i + x_a)^{-1} \bmod q$.

1.3 GEO satellite multicast (c, c_i, z_i, s_i) where $1 \leq i \leq n_s$.

1.4 Whenever a satellite join-leave event occurs, key update is realized with ELK protocol using $k_{i,1}$ keys.

2) Key-Ticket Distribution and Data Multicast in LEO and MEO Satellite Layers: Each LEO and MEO satellite uses required (c, c_i, z_i, s_i) tuple to recover group key, group key seeds and data. Private keys sx_i are used for public key generation. Public keys are send to GEO satellite.

2.1 Key generations and transmission: $sx_i = BBS(= n_s)$, $y_i = g^{sx_i} \bmod p$, $GEO \leftarrow y_i$ where $1 \leq i \leq n_s$.

2.2 Unsigncryption Processes: Obtain tuple (c, c_i, z_i, s_i) and $k_i = H((y_a g^{z_i})^{s_i sx_i} \bmod p)$, $k_i \rightarrow (k_{i,1}, k_{i,2})$,

$GK = D_{k_{i,1}}(c_i)$, $w = D_{GK}(c)$ where $w = (M, h)$,

$if(((h == H_{GK}(M)) \wedge (z_i == H_{k_{i,2}}(w)))$ then signcryption is valid. Recover $M = (st_i, sm_i, m_{geo})$.

2.3 Each LEO and MEO satellite (i'th satellite in satellite layers) uses group key seed st_i to generate group key vector $t_{i,j}$ as mentioned above. Whenever a TU join-leave event occurs, satellites use these group keys (elements of $t_{i,j}$) for group key update. For data multicast, satellites may directly pass m_{geo} or add their own multicast data such that $m_{geo} \subseteq m_{leo-meo}$. Also, LEO and MEO satellites generate validation tickets for usage of MMUs. Validation tickets are stored to response many-to-many multicast requests of MMUs. Note that, which TU is managed by which satellite is determined by an appropriate satellite internetworking mechanism like [20]. Each LEO and MEO satellite performs following steps:

$t_{i,j} = BBS(st_i)$, $1 \leq i \leq n_s$, $j \geq n_m$, $stc_i = BBS(\geq n_m)$. Public-private key generations are similar to step 1.1 in GEO satellite layer.

2.4 Each LEO and MEO satellite uses public keys of their related TUs (p', q', g', y_a') and performs following operations:

$GK' = t_{i,j}$, $M' = (stc_i, sm_i, m_{leo-meo})$,

$h' = H_{GK'}(M')$, $c' = E_{GK'}(M', h')$, $k_i' = H(y_i^{v_i'} \bmod p')$,

$k_i' \rightarrow (k_{i,1}', k_{i,2}')$, $c_i' = E_{k_{i,1}'}(GK')$,

$z_i' = H_{k_{i,2}'}(M', h')$, $s_i' = v_i'(z_i' + x_a')^{-1} \bmod q'$.

2.5 Each LEO and MEO satellite multicast their (c', c_i', z_i', s_i') tuple where $1 \leq i \leq l$.

2.6 Whenever a TU join-leave event occurs, key update is realized with ELK protocol using $k_{i,1}'$ keys. LEO or MEO satellite realizes key update such that $t_{i,j} \rightarrow t_{i,j+1}$ and GEO satellite is informed for local group key update.

2.7 If many-to-many multicast requests come from MMUs or TUs, firstly LEO satellites, and if they are not available then MEO satellites validate tickets of MMUs or TUs. If ticket is valid then many-to-many multicast requests are performed. Validation mechanisms are mentioned at lower layers. Note that, tickets are also used to assign one of the MMU if TU of that local region is not available.

3) Key-Ticket Distribution and Data Multicast in TU Layer: TUs are mainly responsible for decrypting required keys and multicast data coming from satellite layers and multicast them in encrypted form using group key seeds sm_i for MMUs or members. Group key seeds and multicast data $m_{leo-meo}$ are recovered from (c', c_i', z_i', s_i') by each TU using SCS1M algorithm.

3.1 Public-private key pair generations are similar to the upper layers. Each TU performs following steps:

$k_i' = H((y_a' g'^{z_i'})^{s_i' sx_i'} \bmod p')$, $k_i' \rightarrow (k_{i,1}', k_{i,2}')$,

$GK = D_{k_{i,1}'}(c_i')$, $w' = D_{GK'}(c')$ where $w' = (M', h')$,

$if(((h' == H_{GK'}(M')) \wedge (z_i' == H_{k_{i,2}'}(w')))$ then signcryption is valid. Recover $M' = (stc_i, sm_i, m_{leo-meo})$.

3.2 Each TU generates ticket vector tc_i using ticket seed stc_i and generates $m_{i,j}$ group key vector using group key seed sm_i.

3.3 TU prepares data packets including $M'' = (m_{leo-meo}, tc_i)$ for its local MMU and member group and transmits these values to them. Like upper layers, M'' is signcrypted using public keys of the MMUs and members that TU manages together with $m_{i,j}$.

3.4 Whenever a member or MMU join-leave event occurs, key update is realized with ELK protocol using $m_{i,j}$ group keys. TU realizes group key update such that $m_{i,j} \rightarrow m_{i,j+1}$ and LEO or MEO satellite is informed for group key update.

1-4244-0357-X/06/$20.00 ©2006 IEEE

3.5 TUs evaluate many-to-many multicast requests of MMUs and members for local group without ticket requirement. For many-to-many multicast requests covering MMUs or members groups, which are related to other TU local groups, are evaluated using tc_i tickets. tc_i tickets are send by MMUs using $m_{i,j}$ key of MMU. For this part of the SSMS, authentication may be provided by either $MAC(D_{m_{i,j}}(tc_i))$ using MAC (Message Authentication Code) or challenge response mechanisms which can utilize secret keys. Also, it is possible to use SCS1M for this purpose. Then, TU redirect validated multicast data and tickets to the LEO or MEO satellites. With same mechanism, LEO or MEO satellites decide whether many-to-many multicast requests are valid or not. If they are valid then, like original multicast data, many-to-many multicast data are done to related parts of the system.

4) Data Multicast and Member Management in MMU and Member Layers: MMUs are used to provide reliability in terrestrial layers. Especially for military applications, if TUs are not available, then using ticketing mechanism, one of the MMU is assigned as local group manager. Also, MMUs are required to support mobile light-weight members that TU can not cover for various reasons. Many-to-many multicast requests of members are generally provided by MMUs using ticket mechanism via TUs, LEO or MEO satellite as mentioned at upper layers.

V. Performance Analysis of NAMEPS

We analyze NAMEPS for two major criteria in details: Bandwidth consumption and computational workload. For these analyses, we firstly compare NAMEPS for cryptographic primitive aspect with other traditional approaches. Secondly, we analyze advantages of architectural design and key management method used in NAMEPS focusing on two major criteria. Using these analyses, we give our simulation results comparing NAMEPS with pure implementation of LKH, OFT, ELK protocols and TTPVSS protocol.

Apart from these, NAMEPS provides advantages for storage requirement. N-tier architecture of NAMEPS reduces number of keys that are stored in both satellite and terrestrial layers. Each group manager in SSMS only stores keys for their related members. For satellites, they only store keys for their related TUs and MMUs ($\approx (2l + n_m)$). In pure implementations of LKH, OFT and ELK, satellite stores a unique key for each member, in total n keys. Thus, significant storage advantage is obtained. Also,when compared with TTPVSS, NAMEPS has advantage due to the satellite internetworking possibilities.

A. Advantages of SCS1M Usage in NAMEPS

In SSMS, traditional PKC (Public Key Cryptography) methods such as DH (Diffie-Hellmann), ECDH, factorization based and DLP based signature schemes together with their extensions of EC domains are used [21], [22]. NAMEPS uses SCS1M as major cryptographic primitive for PK data transmission. Thus, NAMEPS utilizes all advantages of signcryption based methods and especially SCS1M when compared with the traditional cryptographic primitives used in SSMS.

SCS1M has significant computational and communication overhead advantages when compared with classical DLP and factorization based signature approaches: For sender, SCS1M reduces number of exponentiations and saves from computational cost by a factor larger than 50%. For recipient, SCS1M uses Shamir's fast exponentiations of the product of the exponentials and saves from computational cost by a factor 45%. Most significant gain is obtained for communication overhead. Note that, this criterion is the most important criterion for SSMS. For $|p| = 1024$ and $|q| = 160$, SCS1M provides communication overhead advantages up to 81%. Communication overhead gain increases when $|p|$ and $|q|$ increase. Saving for communication overhead is larger for RSA based key management approaches. Details can be found in [14], [15]. Note that, DLP signcryption methods can be extended to EC domain [16]. Thus, advantages of NAMEPS are also valid for comparisons of ECC based traditional approaches.

In simulation results, we reflect aforementioned advantages of SCS1M to the classical approaches as cryptographic workload coefficient (CWC). CWC for SCS1M, TTPVSS and traditional methods are represented with c_1, c_2 and c_3 respectively. Following inequality holds: $c_1 \cong c_2 < c_3$.

B. Advantages of Architectural Design and Properties of NAMEPS

In NAMEPS, N independent key distribution layers provide major performance gain. In each layer, whenever a member join-leave event occurs, in order to provide forward and backward security, key update (rekeying) is realized on only related part of the layer and other parts of the SSMS are not affected from these processes.

Rekeying workload is the most important parameter that determines overall performance of SSMS. Rekeying workload is determined by number of join-leave events for certain time period, r, and cost of the rekeying operation. Cost of the rekeying operation depends on the cost of the applied key management protocol (ELK in each layer for NAMEPS) and cryptographic costs of the used cryptographic primitives (c_1, c_2 and c_3 for NAMEPS, TTPVSS and others, respectively). Using these facts, we calculate rekeying workload of the related group manager (satellite, TU or MMU) according to the number of members it manages, number of rekeying, cryptographic cost, communication overhead and cost of the core key management protocol for key update operation. We refer total cost of the rekeying taking into consideration these parameters as TRBCC (Total Rekeying Bandwidth-Cryptographic Cost).

In NAMEPS, for each key update, ELK protocol is applied in related layers. As mentioned in section II, ELK provides smaller packet size and super-efficient member join when compared with many other protocols. For single member join, ELK does not cause rekeying workload. For member leave, ELK requires $log_k n\,|K|$ where n is the number of members that ELK protocol is applied, k is the branching factor of the logical key tree, and $|K|$ bit length of the ELK keys. However, in LKH and OFT protocols, both member join-leave operations causes rekeying workload larger than ELK leave event cost

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

(join does not create cost) such that $(klog_k n - 1)\,|K|$ and $(log_k n - 1)\,|K|$, respectively. Note that, generally, $|K'| \leq |K|$.

Most resource limited components of the SSMS is satellite layers. Thus, we specifically analyze workload of these layers. Note that, analysis principles are the same for terrestrial layers. Each satellite manages a TU group having l_t TU on average. Whenever a TU join-leave event occurs, satellite realize rekeying with cost $c_1 \log_k l_t\,|K'|$. TU join events do not create workload. r_s is the number of rekeying for TU layer, $Pr(leave)$ is probability that occurred event is a leave event. Note that, TUs are generally static components, thus $r_s << r$ where r is number of join-leave events for all member (rekeying workload for overall system).This provides significant performance gain for NAMEPS when compared with pure implementations of LKH, OFT and ELK protocols. Moreover, properties of SCS1M and abilities of the large satellite internetworking provide better batch keying, represented with m_1. This also reduces workload of the satellite layers in NAMEPS when compared with TTPVSS protocol, and pure implementations of LKH,OFT and ELK protocols. Moreover, in NAMEPS, a ticketing mechanism is used that make system more resistant against single point of failure problems. Also, with ticketing mechanism, MMUs can directly contact with satellites and can realize many-to-many multicast, even if their join-leave events does affect to the satellite layer. As a result, TRBCC for satellite layer is $c_1 \log_k l_t\,|K'|\,r_s \Pr(leave)/m_1$.

In TTPVSS, like NAMEPS, satellite is not affected from overall member join-leave rekeying workload, which is r. Thus, TTPVSS has a significant advantage to pure implementations of the LKH, OFT , and ELK protocols. TTPVSS uses LKH protocol in each of its layers. When compared with NAMEPS, in TTPVSS, a satellite is responsible for all TUs . Also, due to no ticketing mechanism is used, MMUs are also managed by satellite which increases number of components that satellite is responsible for, $((l + n_m) >> l_t) \Leftrightarrow (r_{(l+n_m)} >> r_s)$. Moreover, for batch keying value of TTPVSS, $m_2 < m_1$. Thus, TRBCC for satellite in TTPVSS is $c_2 \log_k(l + n_m)\,|K|\,r_{(l+n_m)}/m_2$.

In pure implementations of LKH, OFT and ELK protocols, group manager is directly responsible for all members, thus parameter r affects the satellite. This causes massive workload over satellite. In addition to this, in previous protocols, only TUs or MMUs involve core key management protocol cost. However, in this situation, $n >> n_m > l$ and significant workload occurs for satellite. In pure implementations, no specific batch keying or ticketing mechanism is used. Thus, TRBCC for satellite in LKH, OFT and ELK protocols are $c_3(k \log_k n - 1)\,|K|\,r$, $c_3(\log_k n + 1)\,|K|\,r$ and $c_3 \log_k n\,|K'|\,r \Pr(leave)$.

As a result, following TRBCC relation exists among pure implementations of LKH, OFT, ELK protocols and TTPVSS and NAMEPS protocols respectively:

$c_3(k \log_k N - 1)\,|K|\,r > c_3(\log_k N + 1)\,|K|\,r > c_3 \log_k N\,|K'|\,r \Pr(leave) >> c_2 \log_k(l + n_m)\,|K|\,r_{(l+n_m)}/m_2 >> c_1 \log_k l_t\,|K'|\,r_s \Pr(leave)/m_1$ where $r >> r_{(l+n_m)} >> r_s$ and $c_1 \cong c_2 > c_3$.

We can clearly see that, NAMEPS is the most efficient protocol among these protocols for most important criteria.

C. Simulation Results

Simulation results are based on the evaluation of the satellite layers for TRBCC measurements. In the first simulation(fig. 1), TRBCC responses of protocols for increasing members sizes for certain member rekeying value (r) are analyzed. We use rekeying ratio coefficient $rrc = 0.25$. In certain time period, $r = n * rrc$ rekeying occurs. TRBCC values of satellite layers for $n = 10^5 \rightarrow 10^7$ are calculated. Rekeying behavior of r and TU-MMU join-leave events obey Poisson rule. Other parameters are taken according to the aforementioned criteria.

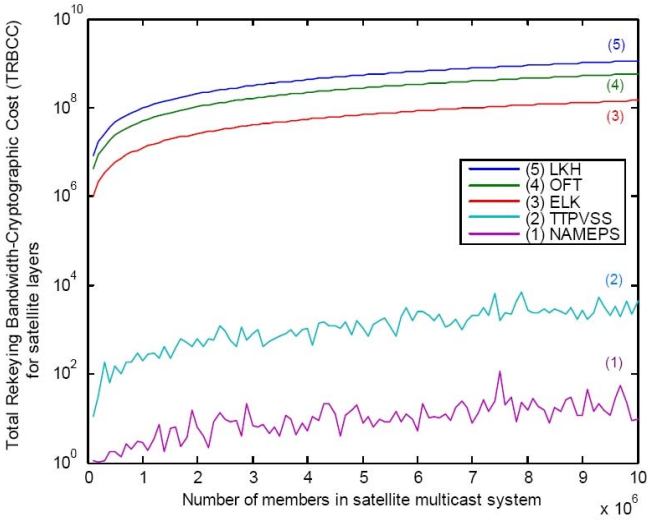

Fig. 1. TRBCC comparison of NAMEPS for increasing member size

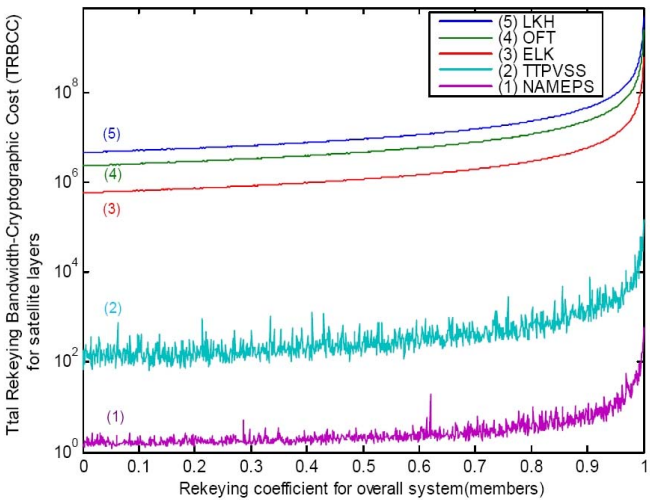

Fig. 2. TRBCC comparison of NAMEPS for increasing member dynamism

In second simulation (fig. 2), we analyze TRBCC responses of protocols for increasing member dynamism, which is number of members join-leave for certain time period, for certain number of members. $n = 10^7$, $rrc = 10^{-3} \rightarrow 1$ and

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

TRBCC workload of satellite layers are observed. Randomized behaviors obey Poisson rule similar to above.

As a result, we can clearly see that NAMEPS has lowest workload among the pure implementations of LKH, OFT, ELK protocols and TTPVSS protocol. NAMEPS and TTPVSS have significantly lower TRBCC workload than pure implementations of LKH,OFT and ELK. NAMEPS also has significant performance advantages to TTPVSS for aforementioned reasons. Simulation results show that NAMEPS can be applied extremely large multicast groups without having performance and security problem. Also, dynamism response of NAMEPS is very promising.

Possible disadvantages of NAMEPS seem to be its complexity and network associated delay problems. But, integration of N-tiered satellites and terrestrial networks is inevidible within the concept of next generation network systems. Thus, NAMEPS is especially suitable for these networks. Also, since bulk data communication is performed by symmetric cryptography, delay problem will be neglible. In our future works, we will exploit these issues.

VI. Conclusion

In this paper, we propose a new satellite multicast security protocol using N-tiered architecture based on multi-recipient signcryption schemes. NAMEPS uses N independent key distribution layers to provide significant performance gain for especially satellite layers. Effects of the group key update operations resulting from member join-leave events are restricted on only local parts of the related layers. This approach significantly reduces rekeying workload and number of keys that are stored in satellite layers as well as terrestrial layers. Also, batch keying, validation ticket and N-tier satellite internetworking mechanisms are used that additionally reduces rekeying workload and provides reliability for SSMS. NAMEPS uses ELK protocol in each of its layer providing advantages for rekeying costs and packet sizes. Apart from architectural design, as a novelty, NAMEPS uses multi-recipient signcryption schemes (SCS1M) as a major cryptographic primitive for key management in SSMS. Using SCS1M, NAMEPS has all advantages of signcryption based schemes to the classical sign-then-encrypt approaches as well as utilizing additional benefits of multi-recipient version. We analyze and compare NAMEPS with the pure implementations of LKH, OFT and ELK protocols and TTPVSS protocols. Simulation results are given based on the analysis and comparison of these protocols for TRBCC values. We can clearly see that NAMEPS is the most efficient protocol for major criteria such as bandwidth consumption, cryptographic workload and number of keys that are stored in components of the SSMS among mentioned protocols. As a result, NAMEPS is especially suitable for very large and dynamic satellite multicast system requiring high security and provides significant advantages when compared with the some well-known protocols.

Acknowledgment

This work is supported by the State Planning Organization of Turkey under “Next Generation Satellite Networks Project”, and Bogaziçi University Research Affairs.

References

[1] D. H. S. Rafaeli. A survey of key management for secure group communications. ACM Comp. Surveys, vol. 35, no. 3, Sept 2003, pp. 309–29.

[2] M. P. Howard, S. Iyengar, Z. Sun, H. Cruischank. Dynamics of key management in secure satellite multicast. IEEE Journal on Selected Areas in Communications, Vol. 22, No.3, Feb 2004.

[3] A. Menezes, P. Van Oorschot, and S. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[4] D. Wallner, E. Harder, and R. Agee. Key management for multicast: Issues and architectures. IETF, RFC2627, June 1999.

[5] D. Balenson et al. Key management for large dynamic groups: One way function trees and amortized initialization. IETF Draft, work-in progress, draft-balenson-groupkeymgmt-oft-00.txt, February 1999.

[6] Alan T. Sherman , David A. McGrew, Key Establishment in Large Dynamic Groups Using One-Way Function Trees, IEEE Transactions on Software Engineering, v.29 n.5, p.444-458, May 2003.

[7] A. Perrig, D. Song, and J.D. Tygar. ELK, a new protocol for efficient large-group key distribution. IEEE Security and Privacy Symposium May 2001.

[8] S. Mittra. Iolus: A framework for scalable secure multicasting.In Proceedings of the ACM SIGCOMM’97, September 1997.

[9] S. Setia, S. Koussih, and S. Jajodia. Kronos: A scalable group rekeying approach for secure multicast. In Proceedings of the IEEE Symposium on Research in Security and Privacy, May 2000.

[10] J. Huang and S. Mishra. Mykil: A highly scalable and efficient key distribution protocol for large group multicast. In the IEEE 2003 Global Communications Conference (GLOBECOM 2003), San Francisco, CA (December 2003).

[11] A. Altay Yavuz, F. Alagoz , E. Anarim. A new satellite multicast security protocol based on elliptic curve signatures. IEEE International Conference on Information Communication Technologies (ICTTA’06) , April 2006.

[12] A. Altay Yavuz, F. Alagoz, E. Anarim. Three-Tiers satellite multicast security protocol based on ECMQV and IMC methods. IEEE Computer-Aided Modeling, Analysis and Design of Communication Links and Networks (CAMAD’06), June 2006.

[13] W. Mao. Modern Cryptography Theory and Practice. Hewlett-Packard Company, Prentice Hall, 2004.

[14] Y. Zheng. Shortened digital signature, signcryption, and compact and unforgeable key agreement schemes (A contribution to IEEE P1363 Standard for Public Key Cryptography), July 1998.

[15] Y. Zheng. Digital signcryption or how to achieve Cost(Signature and Encryption) $<<$ Cost(Signature) + Cost(Encryption). Advances in Cryptology, Crypto’97, Lecture Notes in Computer Science, Vol. 1294, pp. 165-179, Springer-Verlag, 1997.

[16] Y. Zheng and H. Imai. “How to construct efficient signcryption schemes on elliptic curves. Information Processing Letters, Vol.68, pp.227-233, 1998.

[17] Y. Zheng. Signcryption and its applications in efficient public key solutions. Proceedings of 1997 Information Security Workshop (ISW’97), Lecture Notes in Computer Science, vol.1397, pp.291-312, Springer-Verlag, 1998.

[18] Y. Zheng and H. Imai. Compact and unforgeable key establishment over an ATM network. Proceedings of IEEE INFOCOM’98 , pp.411-418, 29/3-3/4, 1998.

[19] B. Schneier, Applied Cryptography. New York: Wiley, 1996.

[20] C. Chen, E. Ekici, and I.F. Akyildiz. Satellite grouping and routing protocol for LEO/MEO satellite networks. Proceedings of the Fifth ACM WoWMoM, 2002, pp. 109-116.

[21] New Directions in Cryptography. W. Diffie and M. E. Hellman, IEEE Trans. Information Theory, vol. IT-22, Nov. 1976, pp: 644 654.

[22] Standard specifications for public key cryptography. IEEE P1363/D13, 1999.

1-4244-0357-X/06/$20.00 ©2006 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.