ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

A Detailed Survey on Secure Multicast Group Key Management Schemes

P.Vijayakumar[1], L.Jegatha Deborah[1]

[1] Department of Computer Science and Engineering, University College of Engineering Tindivanam, Melpakkam, India- 604 001
E-mail: vijibond2000@gmail.com, blessedjeny@gmail.com

Abstract

In the past, many researchers have worked on centralized multicast key management and key distribution schemes for secure multicast communication which can be applied to many applications such as Pay-TV systems video conferences, sporting events, audio and video broadcasting. However, most of these schemes consume more key computation time and memory and in addition, most existing schemes take more rekeying cost. In this paper a detailed survey is made to analyze the merits and limitations of the key management schemes available in the literature. Moreover, based on the detailed survey, we have also suggested a new key management scheme which would minimize the complexities of the existing key management and key distribution schemes.

1. WORKS ON CENTRALIZED MULTICAST KEY MANAGEMENT

Wallner et al (1998) discussed about the difficult problem of key management for multicast communication sessions. It focuses on two main areas of concern with respect to key management, which are initializing the multicast group with a common net key and rekeying the multicast group. A rekey may be necessary upon the compromise of a user or for other reasons (e.g., periodic rekey). Even though, these authors achieved efficiency in terms of rekeying cost and memory, it must be further enhanced to provide better performance by avoiding delays in packet transmission. Steiner et al (2000) proposed a new key management protocol based on the Diffie-Hellman key exchange. This protocol achieves secure and efficient key agreement in the context of dynamic peer groups which are relatively small and nonhierarchical. Their protocol is efficient only for small groups and not suitable for large groups. Wong et al (2000) presented a novel solution to the scalability problem of group or multicast key management. They introduced the concept of key graphs for specifying secure groups. In addition, they presented three strategies for securely distributing rekey messages after a join and leave and proposed new protocols for joining and leaving a secure group. The rekeying strategies and join and leave protocols have been implemented in a prototype key server that they have built.

Wade Trappe et al (2001) controlled the problem of access on multimedia multicasting which requires that it is necessary to have the key distribution and maintenance information. The conventional approach for distributing keys is to use a channel independent of the multimedia content. They proposed a second approach, which involves the use of a data-dependent channel, and

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

achieved for multimedia by using data embedding techniques. Poovendran et al (2001) showed that the rooted-tree-based secure multicast key distribution schemes can be useful for collision avoidance and reduces memory requirements. Mingyan Li et al (2002) studied the problem of distributing cryptographic keys to a secure multicast group with a single sender and multiple receivers. They showed that the problem of designing key distribution model with specific communication overhead can be posed as a constraint optimization problem. Using the formulation, they showed how to minimize the number of keys to be stored by the group controller. An explicit design algorithm with given key update communication budget was also presented by them. The main advantage of their work is that they provided security for one to many communications. However, the solution to the constraint optimization problem itself is much complex.

Wade Trappe et al (2003) presented two modes of conveyance for transmitting the rekeying messages. By embedding the keying information in the multimedia content, the key updating messages associated with secure multicast key management schemes has been hidden in the data in their work and they used it in conjunction with encryption to protect the data from unauthorized access. The main advantage of all these works is reduction in memory requirements to a certain extent.

David et al (2003) presented and analyzed a new practical centralized hierarchical algorithm for establishing shared cryptographic keys for large, dynamically changing groups. Their algorithm is based on a novel application of One-way Function Trees, taking a bottom-up approach with the option of member contributions to the entropy of the common communications key. Unlike previously proposed solutions based on information theory and hybrid approaches the One-way function algorithm proposed by them has communication, computation and storage requirements that scale logarithmically with group size, for adding or evicting operation.

The problem of designing a storage efficient secure multicast key management scheme based on One-way function trees for a pre-specified key update communication overhead was proposed by Mingyan Li et al (2004). Fei et al (2005) designed a Video-Cassette-Recorder (VCR) friendly broadcast series and proposed an active buffer management technique to implement the functionality of providing interactive services in broadcast Video on Demand (VoD) systems. They showed that their scheme can implement VCR actions through buffering with a high probability in a wide range of user interaction levels. Wang et al (2006) proposed an efficient time-bound scheme based on a technique called Merging. The idea behind merging is to consider primitive keys instead of hierarchies. It is conceptually actually to be like the compression used in source coding. Through this technique, therefore actually it is

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

feasible to combine multiple keys into an aggregate key. Thus, communication and storage requirements are greatly reduced. However, the computation time is high in this approach.

Purandare et al (2007) introduced a novel framework for Peer to Peer (P2P) media streaming, that uses alliance based peering scheme to solve some of the existing problems in chunk based P2P media streaming. In particular, their main contributions are reduction in buffering time and achievement of scalability. Dong-Hyun Je et al (2010) proposed a computation-and-storage-efficient key tree structure, and a key tree management protocol for secure multicast communication. By considering the resource information of each group member's device, this protocol manages the key tree structure to maximize the efficiency of the computation and storage costs and minimizes the increment of the communication cost.

Lihao Xu et al (2008) proposed a new multicast key distribution scheme in which the computation complexity is reduced by using Maximum Distance Separable (MDS) codes to distribute multicast key dynamically. Mahalingam Ramkumar et al (2010) proposed three techniques for key distribution which not only reduce computational complexity but also the bandwidth and storage requirements to some extent. Moreover, they have provided a security model to prevent Message-Injection Attacks.

Naranjo et al (2010) presented a new algorithm for key management in which they explained three applications of their algorithm to security and privacy field. The first one is a method for controlling the disclosure of discrete logarithm-based public keys. It can be used to privately deliver a public key to a set of recipients with only one multicast communication. The second method is an authentication technique that has been used in scenarios where a public-key infrastructure is not available. The third application proposed by them uses the Extended Euclidean algorithm which is a zero-knowledge proof. Moreover, it reduces the number of messages exchanged between the two applications mentioned above. The main limitations of these existing works are the computation complexity involved in rekeying operations leading to decrease in performance. In addition, the memory requirements are high in most existing schemes. Comparing with all these existing schemes, the key management schemes proposed in this paper are more efficient in terms of computation, communication and storage aspects.

1.1 Works on ID Based Key Distribution Using Elliptic Curve Cryptography

A secure communication-efficient key agreement protocol based on the bilinear pairings in Ad hoc Networks was proposed by Hongsong Shi et al (2005). In their protocol, the dynamicity of the networks is considered and the 1-hop assumption is weakened by employing hierarchical routing techniques to ensure that the logical

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

model of key agreement coincides with the actual topology of networks. Wu et al (2005) proposed an ECC pairing-wise, user-friendly remote timestamp-based password authentication scheme with smart cards and its extended version named nonce-based password authentication scheme. These proposed schemes do not use any password file or verification table to authenticate the users. They also analyzed some possible attacks. Their proposed scheme eliminates the drawback of traditional ID-based scheme of assigned un-human lengthy password. The remote distributed hosts need not have the knowledge of the secret key information to authenticate the legitimacy of the user. This enhances the flexibility of the proposed authentication scheme. In addition, the scheme inherits the merits of ECC with small key size and high security. It is especially well suited to smart card applications, mobile communications and other remote distributed systems.

A distributed electronic authentication scheme based on elliptic curve was proposed by Chen et al (2007). This scheme consists of two parts in which the first part is useful for constructing the necessary licenses. The second one can be used for validating license. Because, the security of these licenses are determined by private key, but not the arithmetic itself, any user cannot construct new license by using the given license and the public key, as long as the private key is not leaked. They also analyzed the security. The main advantage of their work is improvement in security and reliability. Jin-Hee et al (2008) proposed an analytical model to address the issue of how often batch rekeying should be performed. They proposed threshold-based batch rekeying schemes and demonstrated that an optimal rekey interval exists for each scheme. They compared these schemes to identify the best scheme which can minimize the communication cost of rekeying while satisfying application requirements using a set of parameter values characterizing the operational and environmental conditions of the system. Lee et al (2008) proposed an algorithm that finds one of the candidate tree structures. As an another approach, in order to determine a definite optimal tree structure, they also proposed a new cost metric that considers member dynamics as well as the average number of rekeying messages.

Chun-I Fan et al (2010) presented an anonymous multi receiver identity-based encryption scheme where they adopted Lagrange's interpolating polynomial mechanisms to cope with the above problem. Their scheme is more complex for an attacker to derive the identity of the message receiver in such a way that the privacy of receivers can be guaranteed. Furthermore, their scheme is quite receiver efficient since each of the receivers merely need to perform twice of pairing computation to decrypt the received cipher text. They also proved that their scheme is secure against adaptive chosen plaintext attacks and adaptive chosen ciphertext attacks. Finally, they have formally shown that every receiver in the scheme is anonymous to any other receiver. Mohsen Imani et al (2010) presented a secure

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

method of the Dynamic Source Routing (DSR) algorithm. This method provides forward and backward security. Compared to the existing methods, their proposed method, which includes proper forward and backward security, is far more secure. They used the cumulative MACs and single MACs to protect the DSR protocol from some well known attacks against it.

Pinaki Sarkar et al (2011) discussed the security characteristics unique to Hierarchical Wireless sensor Networks (HWNs) and showed that how attacks against single or multi-hop wireless networks can be translated into powerful attacks against HWNs. They investigated various types of attacks against HWNs and provided an overview of existing solutions for security protection. They also identified underlying challenges in securing HWNs infrastructure and protecting the transmitted information. Jen-Ho Yang et al (2008) proposed a Dynamic Virtual Digraph (DVD) model for public key distribution. In their work, they have developed a new key distribution scheme by extending graph theory. They proposed the key distribution scheme for pocket based on two-channel cryptography. Tianhua Liu et al (2010) proposed an ID-based remote mutual authentication with key agreement scheme on ECC. Moreover, they adopted multi-servers to realize the scheme's scalability. Compared with existing works, the proposed key distribution scheme is more efficient. The proposed method is more secure and free from attacks. In addition, the method is computationally efficient and consumes only limited memory.

1.2 Key Distribution for Pay TV System

In Pay-TV systems, the service providers are providing various channels to the subscribers based on their choice and payment. In such a scenario, the service provider must use the Conditional Access System (CAS) to restrict the access to unauthorized users and hence needs efficient key management schemes. Tu et al (1999) proposed a simple and a complete scheme of four levels of key hierarchy in the key distribution management for CAS on Pay-TV system. They analyzed the performance of their proposed scheme. Their system is efficient and is suitable for a Pay-TV system which provides both PPC (Pay-Per-Channel) and PPV (Pay-Per-View) services. Their scheme is also a flexible one for dynamic management. However, their focus is on Pay-TV only and hence their schemes are suitable for Digital Broadcasting System (DBS) alone.

Huang et al (2004) presented three key distribution schemes for channel protection and secure media delivery in Pay-TV systems. With their proposed schemes, encryption keys of the subscribed programs have been efficiently and securely distributed to the authorized subscribers. This is because only one message is needed to renew key in the key distribution schemes for subscription channel protection. In addition, they used simpler computation functions, including One-way hash function and Exclusive-OR operation, for key updates to reduce the

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

computation cost. With their key distribution schemes, only authorized subscribers can watch the subscribed programs correctly. Unauthorized subscribers have no facility to retrieve the correct programs over the networks. The main advantage of their work is that service providers can charge their subscribers according to their subscriptions, and the illegal access of the media and video programs from networks can be prevented, based on their proposed schemes. Jiang et al (2004) proposed a grouping access control scheme adopting four-level key hierarchy for key distribution of CAS in DTV (Digital Tele-Vision) broadcasting. By analyzing and comparing, they showed that their proposed scheme has greatly reduced the computation load of encryption and the quantity of messages transferred for rekeying while maintaining higher efficiency and security for CAS. Moreover, their scheme is more flexible and scalable in processing subscriber's joining and leaving. Moreover, this is very important for service provider to dynamically manage the subscriber. Meanwhile, their system is compatible with the DTV standard, which can be used for both PPC and PPV service and are feasible for practical applications. In the end, with the development of China DTV, their scheme has provided practical reference to the security design in the DTV broadcasting. Jiang et al (2004) proposed an efficient time-bound hierarchical key management scheme based on the use of ECC for secure broadcasting of data.

Sakarindr et al (2007) demonstrated that several attacks can be prevented and mitigated by their proposed security services. They also reported several existing works on SGC (Secure Group Communication) over two types of wireless networks namely wireless infrastructure networks and mobile ad hoc networks. With respect to limited computation capability and scarce wireless channels, these works basically attempted to reduce communication and processing overheads, and to fend off some particular attacks. Elisa Bertino et al (2008) showed that Tzeng's scheme is insecure against the collusion attack and they proposed an efficient key management for Pay-TV system in terms of space and time requirements. Sun et al (2008) proposed an efficient and flexible CAS with a four-level key hierarchy. Their proposed CAS is suitable for Flexible Pay-Per-Channel (F-PPC) with millions of subscribers and hundreds of channels. Their proposed CAS can also be applied to a PPV system with a large-scale environment which will lead to a more efficient and scalable PPV system. Wang et al (2008) proposed three key distribution schemes for the access control of Pay-TV systems. According to these schemes, a CAS can support a number of charging strategies for service providers. This includes the proposal of new methods for adopting a smaller charging unit and also by allowing a subscription of any subset of channels with little communication and computational overhead.

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

QijunGu et al (2009) proposed an efficient key management scheme, namely Key Tree Reuse (KTR), to handle key distribution with regard to complex subscription options and user activities. This system supports subscription activities with one set of keys and hence minimizes the rekeying cost. Jung et al (2010) proposed a new key management scheme that overcomes the limitations of the existing conditional access systems by introducing hash operations and new update mechanisms for group key management.

Comparing with all the works present in the literature for handling security in Pay-TV system, the security schemes proposed in this paper are different and efficient in many ways. First, the proposed key management schemes are computationally efficient due to the use of fast multiplication and key computation techniques. Second, the proposed algorithms are secure due to the use of Euler's Totient function and GCD. Third, the proposed scheme reduces memory requirements by the use of tree based storage structures. Finally, the proposed schemes are communication efficient due to the new schemes for rekeying with reduced cost.

2. WORKS ON BATCH REKEYING

Waldvogel et al (1999) presented the Versa Key middleware framework for secure multicasting. The core of the framework consists of three approaches which has different properties, but rely on the same basic principle. All these existing approaches organize the space of keys that will eventually be assigned to group members in a unique way, without actually generating the keys before they are needed. Only when new group keys need to be established, they are generated and distributed to only the members of the group affected by a change. Their organization of the key space assures that all operations on groups are executed with a complexity of O(log n) or less, where n is the size of the group in which the complexity is measured based on the size, number of messages exchanged and the number of cryptographic operations to be performed by any of the participants.

Wong Steve Li et al (2001) presented a new technique for multicast batch rekeying. This technique reallocates the tree nodes in order to keep the tree balanced all the time. Adrian Perrig et al (2001) introduced Efficient Large-group Key distribution (ELK), an efficient, scalable, secure method for distributing group keys. This technique has widespread applications, such as access control in streaming multimedia broadcasts.

Brian Zhang et al (2003) presented the design and implementation of a new key management protocol that is scalable and reliable with respect to performance. The protocol is based upon the use of key trees for secure groups and periodic batch rekeying. At the beginning of each rekey interval, the key server sends a rekey message to all users consisting of encrypted new keys (encryptions, in short) carried in a sequence of packets. They presented a scheme for identifying keys, encryptions, users and a key assignment

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

algorithm that ensures that the encryptions needed by a user are in the same packet. Their protocol provides reliable delivery of new keys to all users eventually. It also attempts to deliver new keys to all users with a high probability by the end of the rekey interval. For each rekey message, the protocol runs in two steps: a multicast step followed by a unicast step. Proactive based Forward Error Correction (FEC) multicast is used to reduce delivery latency.

Onen et al (2004) proposed a new algorithm to separately regroup members into two categories as volatile and permanent members. A threshold value *w* sets the time at which a volatile member is considered permanent. In order to offer higher reliability to permanent members, the key server adjusts the rekeying intervals *Tv* and *Tp* of the respective two sets after computing their corresponding rekeying cost. The proposed protocol fits well for applications where there exists a strong requirement for backward and forward secrecy and where clients pay only for the amount of time they were present in the multicast group. Goshi et al (2003) proposed a height-balanced 2-3 tree (B-tree of order m=3) and found that it has the best performance among the balancing strategies tested. However, balancing a B-tree (Goshi et al 2003) after member joining involves splitting oversized tree nodes and results in worst-case rekeying cost. Haibin Lu (2005) developed a Non-Split Balancing High-Order (NSBHO) tree. Unlike the B-tree scheme, their NSBHO tree does not use node splitting to balance the tree. Their experiments confirmed that the NSBHO-tree is superior to the B-tree in terms of the worst-case rekeying performance. In addition, it has better average-case rekeying performance.

Hock Desmond Ng et al (2007) presented two merging algorithms that are suitable for batch join events. To additionally handle batch depart requests, they have extended these two merging algorithms into a batch balanced algorithm. All three algorithms try to minimize the difference in height of the key tree without adding extra network costs. However, all of the algorithms require the GC to update the affected members on their node position by using update messages. By minimizing the differences in height, they minimized the number of key storages and decryptions needed by each member. This is critical for terminals with limited computation and storage. Furthermore, reducing the number of decryptions helps to reduce the energy consumption, which in turn leads to battery saving.

Lee et al (2008) proposed an algorithm that finds one of the candidate tree structures. As an another approach, in order to determine a definite optimal tree structure, they also proposed a new cost metric that considers member dynamics as well as the average number of rekeying messages. A novel hardware or software architecture was proposed by Abdulhadi Shoufan et al (2009), which optimizes the rekeying performance not only by minimizing the number of cryptographic operations, but also by reducing the execution time of these operations

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

including digital signing with the aid of hardware acceleration. In their system, all help-keys are generated, managed, and stored on hardware, which enhances the system security. To keep flexibility, control-intensive tasks such as tree management are performed as software functions on the embedded processor. The presented rekeying processor was designed based on a comprehensive security analysis with the aid of a novel illustration for security threats, requirements, and technical solutions. A performance measurement on a prototype implementation shows that the rekeying processor can join and disjoin members much faster than software solutions besides supporting much larger groups.

Hai-Tao Xie et al (2009) proposed an m-dimensional space geometry sphere rekeying scheme, in which GC generates parent's key by its child's key when member join or leave, so communication cost of GC for rekeying is reduced. When many of members join or leave at the same time, their batch rekeying scheme improves the rekeying performance. By their simulation, they have shown that their scheme decreases communication cost and storage cost, increase new group key distribution efficiency, and improves expansibility of multicast rekeying. Comparing with the existing rekeying algorithms, the batch rekeying algorithm proposed in this paper is more efficient in terms of rekeying cost with respect to best case and worst case scenarios.

3. WORKS ON KEY DISTRIBUTION IN WIRELESS NETWORKS

Chih-Lin Hu et al (2003) devised an adaptive information dissemination mechanism by exploiting the functionality of data broadcasting, to support the dissemination of static and dynamic information services simultaneously. In their design, both static and dynamic information services are subsumed as service groups, i.e., the building blocks with the uniform representation of structure and group popularity thus, the conventional scenario becomes a special case of their framework. Furthermore, in order to tolerate the broadcast traffic dynamics, they designed an online loan based slot allocation and feedback control technique to deal with the adaptation of the service group classification, bandwidth allocation, and broadcast schedule so as to avoid performance degradation. It is shown by the experimental study that their proposed adaptive information dissemination mechanism associated with the online loan based feedback control was able to achieve a substantial reduction of message traffic for dynamic information dissemination in wireless networks.

Dirk Westhoff et al (2006) presented an approach that concealed sensed data end-to-end and still provided efficient and flexible in-network data aggregation. They applied a particular class of encryption transformations and discussed techniques for computing the aggregation functions "average" and "movement detection." They showed that their approach is feasible for the class of "going

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

down" routing protocols. They considered the risk of corrupted sensor nodes by proposing a key predistribution algorithm that limits an attacker's gain and showed how key predistribution and a key-ID sensitive "going down" routing protocol helped to increase the robustness and reliability of the connected backbone.

Min Shao et al (2009) presented a privacy enhanced key management technique for providing security to data centric sensor networks. In their work, they provided multiple levels of privacy based on different cryptographic keys. In addition, they proposed several query optimization techniques based on Euclidean Steiner Tree and Keyed Bloom Filter in order to minimize the query overhead while preserving query privacy. Nahar Sultana et al (2007) proposed and analyzed a scalable and efficient cluster based group key management protocol by introducing identity based infrastructure for secure communication in mobile wireless sensor networks. To ensure scalability and dynamic reconfigurability, their system takes a cluster based approach by which group members are broken into clusters and leaders of clusters securely communicate with each other in order to agree upon a compromised group key whenever there is a member join or member leave operation. Through analysis, they have shown that their protocol has high probability to be resilient for secure communication among mobile nodes. Finally, they clarified that their proposed scheme is efficient for secure positioning of nodes in wireless sensor network. Hui Chen et al (2007) proposed a cache replacement policy, called On-Bound Selection (OBS), that uses both data access and update information. The proposed OBS is inspired by an analytical analysis for a Server-Based Poll-Each-Read (SB-PER) and a Revised Call-Back (R-CB). The OBS provides an upper bound for effective hit ratio and a lower bound for communication cost. The proposed scheme is evaluated and compared with a Least Frequently Used (LFU) replacement policy through extensive simulations.

Yun Zhou et al (2007) proposed a novel key establishment scheme for sensor networks. This scheme uses a t-degree trivariate symmetric polynomial to facilitate the establishment of both Transport Layer Keys (TLKs) and Link Layer Keys (LLKs) between sensor nodes in a two-dimensional space, where each node calculate direct TLKs and LLKs with some logically neighboring nodes and rely on those nodes to negotiate indirect TLKs and LLKs with other nodes. Any two end nodes can negotiate a TLK on demand directly or with the help of only one intermediate node, which can be determined in advance. As for the LLK establishment, two-LAyer Key Establishment (LAKE) is more secured under the node compromise attack with much less memory cost than conventional solutions. Due to the location-based deployment, LAKE is also energy efficient in that each node has direct LLKs with most neighbors without spending too much energy on the establishment of indirect LLKs with neighbors through multihop routing. Qingyu Xu et al (2008) improved Chien's scheme without public key

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

cryptography which is resistant to Yi X et al (2003) three-party collusion attack. The most important is that their scheme is as efficient as Chein's. Lin et al (2006) proposed a new lightweight, Pollution-attack resistant authentication scheme for multicast communication that generates evidence on receivers for validating on a fast, per-packet basis. This approach is effective for preventing Pollution attacks and it provides better performance when it is compared with the other existing works.

Yoon-Su Jeong et al (2008) proposed a key aggregation technique for facilitating the intermediate nodes for aggregating the data more safely. This protocol is more suitable for providing security to multi-tier network architectures and also to establish secure sessions between sensor nodes and gateways. Patrick Tague et al (2009) proposed and evaluated new metrics for quantifying the availability of network services under the presence of malicious nodes and attackers. They proposed an algorithm called Greedy Node capture Approximation using Vulnerability Evaluation (GNAVE) for the identification of compromised users in the network based on a set of control channels that are jammed. They also evaluated the estimation error using the GNAVE algorithm based on false alarm rate as well as miss rates in the identification problem. They discussed various design trade-offs between robustness to control channel jamming and resource expenditure.

Yan Sun et al (2009) proposed a key tree rebalancing algorithm for improving the rekeying performance algorithms in order to provide an effective scheme for the group key management. Furthermore, they presented a practical Location Based Service (LBS) implementation where they used a hierarchical location information coding. Therefore, their system offers a facility for flexible location information access. Their load tests show that their system is highly practical with good efficiency and scalability.

Patrick Tague et al (2009) developed two complementary vulnerability definitions using two approaches namely a set theoretic and a circuit theoretic approach for analyzing the network traffic. They formed a linear programming model for optimizing the network traffic. Baihua Zheng et al (2009) investigated the tradeoff between the performance and confidentiality of the existing signature-based air indexing schemes which are proposed for wireless data broadcast. In their work, they used two new metrics namely false drop probability and false guess probability to provide effective evaluation and comparison.

1) Yue-Hsun Lin et al (2010) presented Small group PKI (Public Key Infrastructure) – less Authenticated Trust Establishment (SPATE) which is a primitive that allows users to establish trust via mobile devices and physical interaction. In this technique, when the SPATE protocol reaches its completion, its participant nodes will have authentic

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

data which can be used by their applications to interact securely for one week. For that work, their leverage protocol as part of a larger system provides facilities for effective, secure and user-friendly collaboration using e-mail, file-sharing and text messaging services.

Mingyan Li et al (2010) studied controllable jamming attacks in wireless sensor networks, which are easy to launch and difficult to detect and confront. The derived solutions to the optimization problems dictate optimal attack and network defense strategies. Of particular interest is the comparison between the case of perfect knowledge and that of lack of knowledge of the attacker and the network about the strategy of each other. In the latter, the attacker and the network respond optimally to the worst-case strategy of the other. Ying Xuan et al (2011) leveraged several optimization problems to provide a complete trigger-identification service framework for unreliable wireless sensor networks. They provided an improved algorithm with regard to two sophisticated jamming models, in order to enhance its robustness for various network scenarios. Theoretical analysis and simulation results are shown by them to validate the performance of their framework.

Mohamed Mostafa et al (2011) proposed a scheme that uses prior deployment knowledge in terms of the energy level carried by each node for developing a polynomial pool based key pre-distribution scheme proposed in in the previous approach. Their work shows that the node energy level observation can be used to control the creation and the selection of polynomial keys hold by this node. For the purpose of evaluating their proposed scheme they applied it on the A3 protocol as one of known topology control protocols. Their proposed scheme avoids the unnecessary key assignment and it reduces the number of active nodes per topology construction that positively reflects on the performance of the whole Wireless Sensor Networks (WSN).

Patrick et al (2011) presented Nymble, a system in which servers can “blacklist” misbehaving users, thereby blocking users without compromising their anonymity. Giorgio Calandriello et al (2011) analyzed the effect of security on the Virtual Circuit (VC) system effectiveness, notably a safety and an efficiency application. They have provided a framework to analyze the performance of secure VC systems, along with schemes that reduce the complexity and the overhead of security. They considered multiple system operation dimensions and identified interdependencies of various factors. They strongly believed that the systematic evaluation of the overall performance is critical, especially for pervasive computing systems that are tightly coupled to their users. As security and privacy are paramount for those systems, yet they incur significant overhead, designs should be validated to show that the secured systems can be effective as envisioned and needed.

Junbeom et al (2011) proposed an access control mechanism that uses cipher text policies which are based on attribute level encryption in order to enforce

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

effective access control policies with efficient attribute and user revocation capability. They provided a fine-grained access control mechanism using dual encryption technique that takes the advantages of the existing techniques on attribute-based encryption and selective group key distribution in each attribute group. They demonstrated how to apply the proposed mechanism to securely manage the outsourced data. Their results are useful for providing security on data outsourcing systems.

4. LITERATURE GAPS

In spite of all these contributions from literature, there are many gaps that are to be addressed for enhancing the security in key management schemes. Most of the systems present in the literature are computationally expensive. However, they can be decrypted with minimum effort. Moreover, the existing schemes have a number of overheads including memory and communication overheads. Therefore, it is necessary to propose new and efficient key management schemes for enhancing the performance of secure multicast communication.

5. CONCLUSIONS

In the past, many researchers have contributed and proposed various key management schemes. Comparing with most of the existing key management schemes that are in the literature, the key management scheme suggested to use (Vijayakumar et al 2014) in this paper is different in many ways. First, the computation complexity of group centre and group user is reduced substantially by minimising the number of arithmetic operations taken by GC and group user. In order to minimise the computation time both in group centre and user side, we have used CRT-based key management scheme. Second, comparing with all the existing batch rekeying algorithms, the batch rekeying or batch updating algorithm used in this paper is more efficient in terms of computation power taken by the group centre and the number of key values stored by group members are also minimised. Finally, the suggested work also reduces the amount of information that needs to be communicated for updating the keys when there is a change in the group membership.

REFERENCES

1. Abdulhadi Shoufan, Sorin, A. and Huss, “High-Performance Rekeying Processor Architecture for Group Key Management”, IEEE Transactions on Computers, Vol. 58, No.10, pp.1421-1434, 2009.

2. Adrian Perrig, Dawn Song, J.D. and Tygar “ELK A New Protocol for Efficient Large-Group Key Distribution”, Proceedings of IEEE Symposium on Security and Privacy Symposium, pp. 247–262, 2001.

3. Baihua Zheng, Wang-Chien Lee, Peng Liu, Dik Lun Lee and Xuhua Ding, “Tuning On-Air Signatures for Balancing Performance and Confidentiality”, IEEE Transactions on Knowledge and Data Engineering, Vol. 21, No. 12, pp. 1783-1797, 2009.

4. Brian Zhang, X., Lam, S., Young Lee, D. and Richard Yang,Y. “Protocol Design for Scalable and

All Rights Reserved © 2015 IJARTET

Reliable Group Rekeying", IEEE /ACM Transactions on Networking, Vol. 11, No.6, pp. 908-922, 2003.

5. Chen, Z.G. and Song, X.X. "A Distributed Electronic Authentication Scheme Based on Elliptic Curve", Proceedings of the Sixth International on Machine Learning and Cybernetics, pp. 2179-182, 2007.

6. Chih-Lin Hu and Ming-Syan Chen, "Adaptive Information Dissemination: An Extended Wireless Data Broadcasting Scheme with Loan-Based Feedback Control", IEEE Transactions on Mobile Computing, Vol. 2, No. 4, pp. 322-336, 2003.

7. Chun-I Fan, Ling-Ying Huang and Pei-Hsiu Ho, "Anonymous Multireceiver Identity-Based Encryption", IEEE Transactions on Computers ,Vol. 59, No. 9, pp. 1239-1249, 2010.

8. David, A., McGrew and Alan T. Sherman, "Key Establishment in Large Dynamic Groups using One-Way Function Trees", IEEE Transactions on Software Engineering, Vol. 29, No. 5, pp. 444-458, 2003.

9. Dirk Westhoff, Joao Girao and Mithun Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation", IEEE Transactions on Mobile Computing, Vol. 5, No. 10, pp. 1417-1431, 2006.

10. Dong-Hyun Je, Jun-Sik Lee, Yongsuk Park and Seung-Woo Seo, "Computation-and-Storage Efficient Key Tree Management Protocol for Secure Multicast Communications", Elsevier, Computer Communications, Vol. 33, No. 6, pp. 136-148, 2010.

11. Elisa Bertino, Ning Shang, Samuel, S. and Wagstaff "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 2, pp. 65-70, 2008.

12. Fei, Z., Ammar, M.H., Kamel, I. and Mukherjee, S. "An Active Buffer Management Technique for Providing Interactive Functions in Broadcast Video-On-Demand Systems", IEEE Transaction Multimedia, Vol. 7, No. 5, pp. 942-950, 2005.

13. Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux and Antonio Lioy, "On the Performance of Secure Vehicular Communication Systems", IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 6, pp. 898-912, 2011.

14. Goshi, J. and Ladner R.E. "Algorithms for Dynamic Multicast Key Distribution Trees," Procedings of ACM Symposium on Principles of Distributed Computing, pp. 243-251, 2003.

15. Haibin Lu, "A Novel High-Order Tree for Secure Multicast Key Management", IEEE Transactions on Computers, Vol. 54, No. 2, pp. 214-224, 2005.

16. Hai-Tao Xie, Zong-Kai Yang, Yu-Ming Wang and Wen-Qing Cheng, "A M-dimensional Sphere Multicast Rekeying Scheme", Communications and Mobile Computing International Conference, Vol. 3, pp. 418-422, 2009.

17. Hock Desmond Ng, W., Howarth, M., Sun, Z. and Cruickshank. H. "Dynamic Balanced Key Tree Management for Secure Multicast Communications", IEEE Transactions on Computers, Vol. 56, No. 5, pp. 590-605, 2007.

18. Hongsong Shi and Mingxing He, "A Communication-Efficient Key Agreement Protocol in Ad Hoc Networks", IEEE International Conference on

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

Wireless Networks, Communications and Mobile Computing , China, pp. 285-291, 2005.

19. Huang, Y.L. Shieh, S., Ho, F.S. and Wang, J. C. "Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems", IEEE Transactions on Multimedia, Vol. 6, No. 5, pp. 760-769, 2004.

20. Hui Chen and Yang Xiao, "On-Bound Selection Cache Replacement Policy for Wireless Data Access", IEEE Transactions on Computers, Vol. 56, No. 12, pp. 1597-1611, 2007.

21. Jen-Ho Yang, and Chin-Chen Chang, "An ID-based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem", Elsevier, Computers and Security, Vol . 28, pp. 138-143, 2008.

22. Jiang, T., Zheng, S. and Liu, B., "Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcast", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 225-230, 2004.

23. Junbeom, H. and Dong Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 7, pp. 1214-1221, 2011.

24. Jung-Yoon Kim and Hyoung-Kee Choi, "Improvements on Sun et al.'s Conditional Access System in Pay-TV Broadcasting Systems," IEEE Transactions on Multimedia, Vol. 12, No. 4, pp. 337-340, 2010.

25. Lee, J.S., Son, J.H., Park, Y.H. and Seo, S.W. "Optimal Level-Homogeneous Tree Structure for Logical Key Hierarchy", Proc. of IEEE Conference on Communication System Software and Middleware Workshop (COMSWARE), pp. 677- 681, 2008.

26. Lihao Xu, and Cheng Huang, "Computation-Efficient Multicast Key Distribution", IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 5, pp.1-10 , 2008.

27. Lin, Y., Shieh, S. and Lin, W. "Lightweight, Pollution-Attack Resistant Multicast Authentication Scheme", *Proc. ACM Symp. Information, Computer, and Comm. Security, pp. 148-156,* 2006.

28. Mahalingam Ramkumar, "The Subset Keys and Identity Tickets (SKIT) Key Distribution Scheme," IEEE Transactions on Information Forensics and Security,Vol. 5, No. 1, pp. 39-51, 2010.

29. Min Shao, Sencun Zhu, Wensheng Zhang, Guohong Cao and Yi Yang, "PDCS: Security and Privacy Support for Data-Centric Sensor Networks", IEEE Transactions on Mobile Computing, pp. 1023-1038, 2009.

30. Mingyan Li, Iordanis Koutsopoulos and Radha Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 9, No.8, pp. 1119-1133, 2010.

31. Mingyan Li, Poovendran, R. and Berenstein, C. "Design of Secure Multicast Key Management Schemes with Communication Budget Constraint", IEEE Communications Letters, Vol. 6, No.3, pp.108-110, 2002.

32. Mingyan Li, Poovendran, R., David, A. and Mc Grew, "Minimizing Center Key Storage in Hybrid

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

One-Way Function Based Group Key Management with Communication Constraints", Elsevier, Information Processing Letters,Vol. 93, No. 4, pp. 191-198, 2004.

33. Mohamed Mostafa, M., Fouad, Mostafa-Sami, M., Mostafa and Ahmed Reda Dawood, "A Pairwise Key Pre-distribution Scheme Based on Prior Deployment Knowledge", Computational Intelligence, Communication Systems and Networks, International Conference, Vol. 1, pp. 184-189, 2011.

34. Mohsen Imani, Mahdi Taheri and Naderi, M. "Security Enhanced Routing Protocol for Ad Hoc Networks", Journal of Convergence, Vol. 1, No. 1, pp. 43-48, 2010.

35. Nahar Sultana, Ki-Moon Choi and Eui-Nam Huh, "Application Driven Cluster Based Group Key Management with Identifier in Mobile Wireless Sensor Network", Future Generation Communication and Networking ,Vol. 1, No.1, pp. 362-367, 2007.

36. Naranjo, J.A.M., Lopez-Ramosz, J.A. and Casado. L.G. "Applications of the Extended Euclidean Algorithm to Privacy and Secure Communications", Proceedings of the 10th International Conference on Computational and Mathematical Methods in Science and Engineering, CMMSE, pp. 702-713, 2010.

37. Onen, M. and Molva, R. "Reliable Group Rekeying with a Customer Perspective," Proc. IEEE Global Telecommunication Conference, Vol. 4, pp. 2072-2076, 2004.

38. Patrick Tague, David Slater, Jason Rogers and Radha Poovendran, "Evaluating the Vulnerability of Network Traffic using Joint Security and Routing Analysis", IEEE Transactions on Dependable and Secure Computing ,Vol. 6, No. 2, pp. 111-123, 2009a.

39. Patrick Tague, Mingyan Li and Radha Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks", IEEE Transactions on Mobile Computing, Vol. 8, No.9, pp. 1221-1234, 2009b.

40. Patrick, P., Tsang, Apu Kapadia, Cory Cornelius and Sean W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks", IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 2, pp. 256-269, 2011.

41. Pinaki Sarkar and Amrita Saha "Security Enhanced Communication in Wireless Sensor Networks using Reed-muller Codes and Partially Balanced Incomplete Block Designs", Journal of Convergence, Vol. 2, No.1, pp. 23-30, 2011.

42. Poovendran, R. and Baras, J.S. "An Information-Theoretic Approach for Design and Analysis of Rooted-Tree-Based Multicast Key Management Schemes", IEEE Transactions on Information Theory, Vol. 47, pp. 2824-2834, 2001.

43. Purandare, D. and Guha, R. "An Alliance Based Peering Scheme for P2P Live Media Streaming," IEEE Trans. Multimedia, Vol. 9, No. 8, pp. 1633-1644, 2007.

44. QijunGu, Peng Liu, Wang-Chien Lee, and Chao-Hsien Chu, "KTR: An Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services", IEEE Transactions on Dependable and Secure Computing, Vol. 6, No. 3, 2009.

45. Qingyu Xu, Mingxing He and Lein Harn, "An Improved Time-Bound Hierarchical Key Assignment

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

Scheme", Asia-Pacific Conference on Services Computing, pp. 1489-1494, 2008.

46. Sakarindr, P. and Ansari, N. "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks", IEEE Wireless Communication, Vol. 14, No. 5, pp. 8-20, 2007.

47. Wong Steve Li, X., Richard Yang, Y., Gouda, M. and Lam, S. "Batch Rekeying for Secure Group Communications", In Proceedings of 10th International Conference on WWW, pp. 525-534, 2001.

48. Sun, H.M., Chen, C.M. and Shieh, C.Z. "Flexible-Pay-Per-Channel: A New Model for Content Access Control in Pay-TV Broadcasting Systems", IEEE Transactions on Multimedia, Vol. 10, No. 6, pp. 1109-1120, 2008.

49. Tianhua Liu and Hongfeng Zhu, "An ID-Based Multi-Server Authentication with Key Agreement Scheme without Verification Table on Elliptic Curve Cryptosystem", International Conference on Computational Aspects of Social Networks (CASoN), pp. 61-64, 2010.

50. Tu, F.K, Laih. C.S. and Tung. H.H. "On Key Distribution Management for Conditional Access System on Pay-TV System", IEEE Transaction on Consumer Electronics, Vol. 45, No. 1, pp. 151-158, 1999.

51. P. Vijayakumar, S. Bose, A. Kannan, "Chinese Remainder Theorem based Centralized Group Key Management for Secure Multicast Communication," IET Information Security, IET, Vol.8, No.3, pp.179-187, 2014.

52. Wade Trappe, Jie Song, Poovendran, R. and Liu, K.J.R. "Key Distribution for Secure Multimedia Multicasts via Data Embedding", Acoustics, Speech, and Signal Processing, IEEE International Conference on, Vol. 3, pp. 1449-1452, 2001.

53. Wade trappe, Jie song, poovendran, Radha and Ray Liu, K.J. "Key Management and Distribution for Secure Multimedia Multicast", IEEE Transactions on Multimedia, Vol. 5, No. 4, pp. 544-557 , 2003.

54. Waldvogel, M., Caronni, G., Sun, D., Weiler, N. and Plattner, B. "The Versakey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, Vol. 17, No.8, pp. 1614-1631,1999.

55. Wallner, D.M., Harder, E.J. and Agee, R.C. "Key Management for Multicast: Issues and Architectures", Internet Draft Report, Filename: draft-wallner-key-arch-01.txt, 1998.

56. Wang, S.Y. and Laih, C.S. "Efficient Key Distribution for Access Control in Pay-TV Systems", IEEE Transactions on Multimedia, Vol. 10, No. 3, pp. 480-492, 2008.

57. Wang, W.Y. and Laih, C.S. "Merging: An Efficient Solution for a Timebound Hierarchical Key Assignment Scheme," IEEE Transactions on Dependable Secure Computing , Vol. 3, No. 1, pp. 91-100, 2006.

58. Wong, C., Gouda, M. and Lam, S. "Secure Group Communications using Key Graphs", IEEE/ACM Transactions on Networking, Vol. 8, pp.16-30, 2000.

59. Wu, S.T., Chiu, J.H. and Chieu, B.C. "ID-Based Remote Authentication with Smart Cards on Open

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 10, October 2015

Distributed System from Elliptic Curve Cryptography", Proceedings of IEEE International Conference on Electro Information Technology, pp. 1-5, 2005.

60. Yan Sun, Thomas, F., La Porta and Parviz Kermani, "A Flexible Privacy-Enhanced Location-Based Services System Framework and Practice", IEEE Transactions on Mobile Computing, Vol. 8, No. 3, pp. 304-321, 2009.

61. Yoon-Su Jeong, Ki-Soo Kim, Yong-Tae Kim, Gil-Cheol Park and Sang-Ho Lee, "A Key Management Protocol for Securing Stability of an Intermediate Node in Wireless Sensor Networks", Computer and Information Technology, IEEE 8th International Conference, pp. 471-476, 2008.

62. Yue-Hsun Lin, Ahren Studer, Yao-Hsin Chen, Hsu-Chun Hsiao, Li-Hsiang Kuo, Jason Lee, Jonathan M. McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun and Bo-Yin Yang, "SPATE: Small-group PKI-Less Authenticated Trust Establishment", IEEE Transactions on Mobile Computing, Vol. 9, No.12, pp. 1666-1681, 2010.

63. Yun Zhou and Yuguang Fang, "A Two-Layer Key Establishment Scheme for Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 6, No. 9, pp. 1009-1020,2007.

All Rights Reserved © 2015 IJARTET