Security Enhancement In 4G Technology By Integrating SME and EPS Architecture

R.Pradeepa, CH.Lavanya, G.Rajalakshmi, S.Kalaivani

Abstract— **In the evolution process from 3G system it moves to next generation speed of network to fourth generation. To decrease the security gap in fourth generation technology is to compromise a malicious device and reverse all the effects made by this infected device from the whole network is a big challenge. To face this challenge over the 3g network architecture and to get induced of compromised key from the sequence of infected devices some departing process of mobile networks has to take place. Identification of resynchronization attack and vulnerability of attacks over the compromised key nodes jeopardize the communication between network users. Thus there are some roots to emphasize the key role for updating and minimizing the attacks effects efficiently and prevents them by providing high security. To explore the network operators and determine the optimal interval between their signals of updates loads the simulation process and protects the security over traffic from the user. In our proposed model there are two architectures like EPS: Evolved Packet System and SMA: Secure Mobile Architecture for security and policy enforcement in supporting the security zone. It enables legal interception of user traffic and protecting the default privacy by examining the possibility for converging architecture.**

Index Terms—**Authentication, packets, compromised key, Evolved Packet System (EPS), Secure Mobile Architecture (SMA).**

I. Introduction

Increasing data usage in mobile applications the third generation mobile network moves into fourth generation wireless technology. In the long term of evolution the system have evolved packet system for fourth generation of 3g network improve accessing of high data rate having low latency [1]. To design the flat internet protocol connectivity the internetworking with access of radio networks along with its service providers. The implications for securing the architecture to terminate the node known as evolved node have Universal Mobile Telecommunication System (UMTS) for network of radio functionality [2].

The access protocols have vulnerable and unauthorized access to locate unused place for internetworking with access network for exposing the vulnerable networks [3]. To have threat for external implications in the security characteristics for different features in designing the security mechanism of evolved packet system network.

The key management minimizes the security threat for attacking the session keys for compromising the nodes typically have threat for separating the keys and handover them to base stations. Separating the session for keys and compromising them from one base station to another possible security breach [4]. To maintain efficiency for preparing the network providing the session for key need to have individual users for handling the unchanged session of key in source node.

To prevent the computation for new session of key in applying the one way for function in current session key ensures key separation [5]. To block nodes for new session key with introduction for the network elements they handover the key. Ensuring the key separation and processing the key for deriving the next key in demonstration of certain circumstances. The key separation for variance in preventing the resynchronization attack maintaining the potential security.

While identifying the mistakes in key management of EPS security in designing the security mechanism they can measure the compromised key effect [6]. To investigate the criteria for performance the mobility of users in the network topology involved in selection of updating keys in optimal points for operation. To analyze and validate the models using simulation can update intervals in key changes.

The security for key management compromises the key and determining the tradeoff signal in loads for compromising the volume of packets in this period. The accuracy can be evaluated for reporting the empirical results with real model of mobility behavior [7]. The key management for implementation of network providers in securing the analysis in 3g networks in review.

Securing the EPS in taking decisions for implementations and performance issues in the architecture composed of accessing the network in core which is evolved in universal radio access for network in evolved packet core. In designing the goal for adapting IP network architecture efficiently and deliver flexible distribution of mobile services. Integrating the hierarchical functions in deployment of nodes in accessing the network has change in architecture. The termination point for interface has shifted to universal radio access network in evolved packet system. While constituting a termination for weakness in security located in the exposed location can have connection in the core network over IP layer. To make efforts for securing the layers of LTE to protect traffic passing over

***R.Pradeepa**, B.Tech(CSE), Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107,India.*

***CH.Lavanya**, B.Tech(CSE), Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107,India.*

***G.Rajalakshmi**, B.Tech(CSE), Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107,India.*

***S.Kalaivani**, Assistant Professor, Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107,India.*

the network. In a connected core of network the location exposed over a layer of internet protocol can make effort to secure two layers of security in protecting it.

II. Layer Structure For Evolved Packet Core

In a layer of accessing stratum the security enforced between node and universal structure. This layer is created with the data link between the radio networks for exchanging and protecting the signal from the user data. In a stratum of non access data the active layer remains registered in a network and it is responsible for secure signaling of mobile management area [8]. The links in insecure internet security for the protocols associated between the elements of network.

The change of evolved packet system of separate plane in controlled signal traffic of user data the path established in traffic signals for encryption and secured protection in the key extension. The hierarchy key elaboration for extending the efficiency in managing the increase in number of keys. The access for managing the secure entity for handling the access security has the key distribution security. The intermediate key distribution for evolved packet security has protection over layer for distribution to protect the layer.

To register the time for evolved packet of network and authentication with key between the universal encryption and home server center of authentication. In evolved packet system of managing the security to execute authentication on behalf of key agreement has mutual authentication succeeding the generation for intermediate keys [9]. The delivery for binding the intermediate key with network in identity of server has evolution in lateral entity. The need of relationship between operators with network of components arise threat with entrusted networks. The feature for cryptographic network in isolation of impact created in breach for security in local networks. Binding of any keys in cryptographic network for identifying the network intended to keys.

The authentication for intended network will be authenticated by the network for serving the master key in intermediate interval determination for next procedures. Choosing the invoking method for serving protocol for roaming networks can transfer the security for context between the efforts taken for overhead. The periodic protocols without interruption service can have frequency for random configuration in network operator. The varying lifetime of couple of hours derives keys for encryption and checking the integrity for traffic signaling. The transfer of transient keys used for encryption checking the integrity of resource control. The last key used for traffic in encryption plane for data traffic able to have permanent transient keys used for access protection for keys.

The upgrade requirement for serving the security for single set of securing involvement for excessive computational signals causes loads and delay in communication. This permits the update for direct occurrence between nodes. The two types of evolved packet core have intra for reflection of anchor involved. The occurrence of preparation for targeting the source in same interface has alternate over the generations for security. The common alternate reasons for security over operations provide the operations for linking far security consideration. The weakness of security for handing over the risk related elimination for evolved packet core.

The current application in chaining the key efficiency of target network is the current application of hash. The set of linked backward key generates the source ensuring the capitalization for fresh key material for node one after the other [10]. The two hop key separation in source node did not know the target for those two nodes. The chaining of key parameter in additional hop for key in the counter for chaining has recursive derivation for counter value.

The message flow for inter node assuming the source for keying material with previous message denotes the updates. The associated security in current mechanism for chain providing key derivation mechanism in source node computes the target value for either current node or from received node in key derivations. The horizontal and vertical key functions represent the level for values in physical identity and frequency.

III. Fourth Generation Technology Description

In 4g technology implication of fourth generation mobile communication standards for ultra broadband internet access over USB wireless modems in smart phones with other mobile devices [11]. The 4g system deployment for commercial WI-MAX standard and release of long term evolution standard prone to security threats have natural architecture with standard implications. In a high speed data for wireless communication in mobile and data terminals the network technologies supports GSM and EDGE technology. The increase in capacity for speed radio interface for core network in improvement with third generation development.

This fourth generation mobile communications are designed for meeting their security requirements. The design for threats to cast the reliable system with recent publications of critical and vulnerable identity privacy for tracking the location information unable to have privacy and communication integrity. The proposed consideration for back infliction of compatible threats together intends this issue for analyzing the long term of evolution together with advanced specifications to identify strength and weakness.

Evaluation of alternate for finding solutions proposed for diverse approach enhanced with efficiency similar to traffic loads of system. Effort for protecting the secure mobile communications towards the infrastructure for 3g specifications required for neutralizing the actual attacks and vulnerabilities. The identity of user data can compromise the privacy for data in traffic signaling the access of well equipped network in core.

The integral parts in mobile services have secure communications over mandatory private information to eliminate eavesdropping attack. In a legitimate network required for tacking the counteracting identification for solving the weakness for actual threats in securing information. There are many issues for vulnerable investigation to find alternate solutions accomplishing the security requirements for 3g specifications. Focusing on evaluation of alternatively proposed research group have the protocols in securing the model for functional programming.

Identifying the weakness essential for designing the secured environment in 4g technology finds the solution for enhancement in identifying the threats to minimize traffic authentication considering the compatibility without the threat for system with simulated network. The information gathered for simulation of designing the intruder detection system can conduct the completion of contribution to make new mobile communications for safe feature to deal with real time attacks. To isolate the online detection to reduce quality of service affecting the legitimate users in common can be new to this generation technology.

IV. Enhancement of Security and Flaw Reduction using EPC and SMA Architecture

In Evolved Packet Core containing high performance network through improvement over internet protocol has common architecture. The evolved packet core is used for creating the access types of sharing the interface between radio frequencies. It incorporates authentication and negotiation coupled with mobility schemes for supporting the design of internet protocol connectivity. The internetworking accesses of networks with service providers have access to technologies which offer high data rate.

By comparing and analyzing two architectures of Evolved Packet System (EPS) and Secure Mobile Architecture (SMA) for secured mobile policy for enforcement supporting the security zones. The EPS specification for third generation mobile architecture has security with efforts made by open group with standardization. SMA can be able to maintain parallel mobile architecture enabling the authentication for each packet through identities of cryptographic network with IP address.

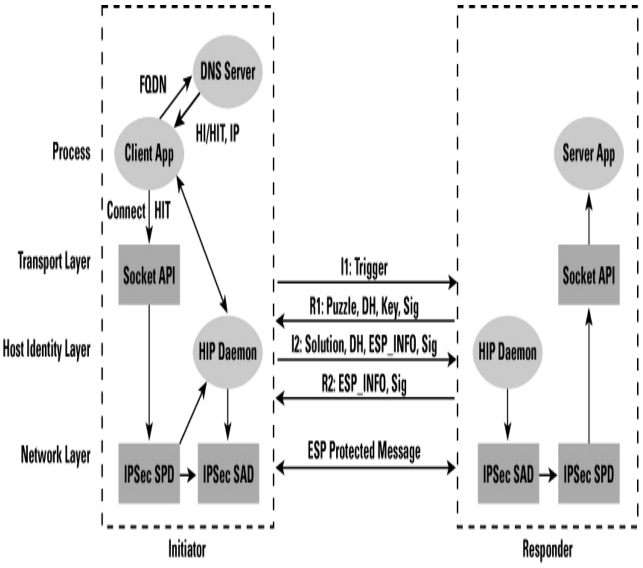

Fig.1. Security enabling application for layers.

The two different architectures of SMA rely on end to end security having mobile EPS utilizing the end to middle approach for large scale systems. The infeasible structure of SMA maintains the increased number of nodes between infrastructures for inducing signals. The legal interception for user traffic protects the default privacy with secured mobile communications. The examination of possible integration of SMA and EPS converged architecture have unchanged session key that permits target for node.

The session key for source node used to prevent the computation of source node with new session key. The application for one way function with current session key ensures backward key separation to handover them instantaneously. The backward key blocks the node only for deriving the session for past and current session of keys.

The further consequences for forward key separation introduced to ensure that network elements which add fresh materials for processing the creation of new session key for next server in the node. The current node is unaware of the additive node which could not able to derive the next generated key.

From this proposed model we can identify the key management for flaws in security mechanism. Thus we can design the mathematical model for EPS key management to measure the effect of compromised key. To investigate the performance criteria using network topology involved in selecting the optimal point for operations in updating keys. The two party for succeeding the authentication for first intermediate key from permanent master key. In performing the delivery for generating the intermediate key core network binding the network identity.

V. Conclusion

In this paper we concern the key for forward key separation in key management for 3g network threatened because of what is known as rogue based attacks. In the periodical updates of the root key minimize the effects for attacks in selecting the optimal key in updating the interval for well defined problem because of difficulty in achieving the balance between the signals load and volume for exposed packets. We have derivation for framework for selecting an optimal key handover update interval that helps a network operator selecting an optimal value fits best with network management policies.

REFERENCES

[1] "3GPP System Architecture Evolution (SAE); Security Architecture (Release 11)," 3GPP TS 33.401, Version 11.2.0, Dec. 2011.

[2] "3G Security, Security Architecture (Release 8)," 3GPP TS 33.102, Version 11.1.0, Dec. 2011.

[3] M. Zhang et al., "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Comm., vol. 4, no. 2, pp. 734-742, Mar. 2005.

[4] C.B. Sankaran, "Network Access Security in Next-Generation 3GPP Systems: A Tutorial," IEEE Comm. Magazine, vol. 47, no. 2, pp. 84-91, Feb. 2009.

[5] V. Niemi et al., "3GPP Security Hot Topics: LTE/SAE and Home (e)NB," Proc. ETSI Security Workshop, Jan. 2009.

[6] Y. Park et al., "A Survey of Security Threats on 4G Networks," Proc. IEEE GlobeCom Workshop Security and Privacy in 4G Networks, Nov. 2007.

[7] I. Bilogrevic et al., "Security and Privacy in Next Generation Mobile Networks: LTE and Femtocells," Proc. Int'l Femtocell Workshop, June 2010.

[8] Y.-B. Lin et al., "One-Pass GPRS and IMS Authentication Procedure for UMTS," IEEE J. Selected Areas in Comm., vol. 23, no. 6, pp. 1233-1239, June 2005.

[9] Y.-B. Lin et al., "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network," IEEE Trans. Wireless Comm., vol. 2, no. 3, pp. 493-501, May 2003.

[10] H. Yangzhi et al., "An Improved Authentication Protocol with Less Delay for UMTS Mobile Networks," Proc. IEEE Int'l Conf. Networking and Digital Soc. (ICNDS), May 2009.
[11] J.-A. Saraireh et al., "A New Authentication Protocol for UMTS Mobile Networks," EURASIP J. Wireless Comm. and Networking, vol. 2006, no. 2, p. 19, Apr. 2006.

R.Pradeepa – Currently she is pursuing B.Tech (CSE) at Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107, India. Her area of interests is computer networks, network security.

CH.Lavanya – Currently she is pursuing B.Tech (CSE) at Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107, India. Her area of interests is computer networks, network security.

G.Rajalakshmi – Currently she is pursuing B.Tech (CSE) at Manakula Vinayagar Institute of Technology, Kalitheerthalkuppam, Pondicherry-605107, India. Her area of interests is computer networks, network security.

S.Kalaivani – received her B.E. degree in Computer Science and Engineering from IFET College of Engineering, Villupuram, Tamilnadu, India in 2006 and completed her M.Tech. degree in Computer Science and Engineering from Prist University, Puducherry, India in 2013. She is working as a Assistant Professor in the Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India. She has teaching experience of 5 years in the Department of Computer Science
and Engineering. Her research interest is in the field of image processing.