Name:

Professor’s Name:

Course:

Date:

Identity Based Cryptography

Abstract

This paper aims to have a comprehensive discussion on identity-based cryptography and a detail explanation on its technical aspect. Moreover, it discusses how IBC has helped in securing the confidentiality and authenticity of information technology specifically in military services through the mobile ad hoc network (MANET). The paper further talks on the challenges encountered in the utilization of identity-based cryptography in the field of telecommunications and information technology.

Introduction

The progressive era of computer systems and telecommunications have call for the pervasive development of technology that prioritizes the security, confidentiality and authenticity of information. Hence, the identity-based cryptography has been invented and is utilized in the world of telecommunication and information technology. Identity-based cryptography is a kind of public-key computerized decoding among openly known string which may represent an individual or an organization. The public string utilized may include an electronic mail address, domain name or IP address. IBC proficiently manages the keying material and supply an easy way of issuing a pair of key applicable to the user‘s key information.

This technology had been introduced in 1984 by Adi Shamir which was purposively used for the verification of digital signatures with the use of public information like the user’s identifiers. Shamir’s identity-based cryptography during that time mainly utilized user distinctive features like e-mail address and phone numbers, unlike today’s system which requires digital certificates for encryption and authenticity verification (Balfe, Boklan & Paterson, 7). That system is much more user-friendly and provides easier access to cryptographers and unprepared users especially that most messages are encrypted for users before it is registered and is generated in any computer systems. Uncomplicated as it was, the IBC of Shamir had not won the interest of the public despite its determination of utilizing the existing RSA function for the identity-based encryption scheme. It was only in 2001 when the research and development of information technology world focused on identity-based cryptography.

Concept of identity-based cryptography

The identity-based cryptography is dependent on the third party called the private key generator (PKG) which can generate either a public or private key pair (indicated by pkPKG or skPKG) and make the pkPKG accessible to the users of the services. The given keys are known as the “master”, and there are two masters – public key and the private key, respectively (Pura & Buchs, 3). The illustration below shows how the encryption and decryption occurs.

The girl sends a plain message M to the boy through the boy's identity IDboy and a PKG to encrypt the message M in a cipher text message C. The boy receives the encrypted message C with instructions of contacting the PKG to obtain the private key in order to decrypt the message. The boy (receiver) authenticates the PKG and provides an adequate proof that indeed the ID belongs to him in which the PKG transmits to him a private key through a protected channel. This channel can be an email address, hence if the user is using an email address then the PKG will be sent through his email. Finally, the boy decrypts the message with the use of the private key in order to recover the plaintext message M send by the girl.

Application in the ad hoc and MANET

The application of the IBC has spread in the field on information technology and is even used in securing the authenticity and confidentiality of messages in the military services. This significant application of IBC is known as the Mobile Ad hoc Network (MANET). This system is characterized by a system of mobile node communication which participates in complex operations to deliver the packet of information from a source node to its destination (Sagheer & Taher, 198). This ad hoc network operates through a secured and protected networks of protocol in order to minimize if not eliminate the environmental threats. Moreover, MANET utilized the identity-based cryptography in order to secure the networks of communication then sends and receives sensitive and confidential messages especially in the military services.

MANET appears to be an essential area for the new invention in the field of information technology especially in wireless communication. The principle of MANET is to make available wireless communication among assorted devices anytime, anywhere without infrastructure. Among the devices where MANET can operate on are cell phones, laptops, remote system and other forms gadgets that can carry out communication with other nodes that are within their frequency range. The participating nodes can either function in message forwarding, information routing, or in authentication of sent and received messages (Sagheer & Taher, 199).

Pura and Buchs (1) cited that the mobile ad hoc network is a recent technology which objective is to provide connectivity between sets of "nodes" in an ad hoc approach. This means that since there is a connection within the network, as long as the nodes communicate then the exchange of messages is possible. In this method there is no need for infrastructure as long as the system utilizes the wireless communication devices. What is necessary is the nodes that direct the exchange of messages. The two nodes within the area can communicate directly or nodes may route the messages along the path for those cases which nodes are not within the area of wireless devices. It can be observed that in the process of sending and receiving messages, security is at risk; hence security issues in telecommunication and information technology are given appropriate treatment. It is here when identity-based cryptography comes in.

In the utilization of the IBC in MANET, the private key generators (PKG) are utilized. Each communicating nodes have been established with encryption keys so that the security and confidentiality, as well as the authenticity of the messages are ensured. The efficiency of the ad hoc networks relies on the packet routing of each participating communication nodes. Among the functions of the packet routing are monitoring of the network traffic, prioritizing the sending of the packets data, authentication of the messages keeping sure that messages come from genuine nodes and keeping track of the routes of messages (Pura & Buchs, 3).

In order to ensure that security is upheld in the communication systems, the participating nodes should share a public-key infrastructure among its users- both the sender and the receiver, respectively. It is necessary that every node generate encryption and signature key pairs and submit certification and other proof of identity to a Certificate Authority (Balfe, Boklan & Paterson, 6).

Challenges of IBC in MANET

Indeed IBC in MANETs have played an important role in securing the information technology system, however, one of its relevant barrier in the public-key decoding is its widespread dependence on the public-key infrastructure that is being shared among its users (Sagheer & Taher, 199).

Another challenge experienced by users of MANET and IBC is the longer time it requires for the processing and submission of the public key, as well as the encryption signature and identity to the Certificate Authority. Youngblood (6) cited also that the process of exchanging and verification of keys and signatures are both time consuming and have the higher possibility of having errors especially for those who are not so familiar of how the ad hoc and identity-based cryptography work. Moreover, Sagheer & Taher (199) cited some other limitations and challenges encountered in the administration of IBC in ad hoc communications, such as lack of preparation, limited interoperability, lack of technical competence in the field of communication and in having limitations in the utilization of the devices.

Related Work

Aside from securing the safety and confidentiality of the messages through the mobile adhoc network, information technology experts have also studied on how they could utilize the routing protocol in detecting misbehaving routers. They have even utilized mobile agent-based mechanism in detecting intruders. There are even new proposals for determining security plan attacks for the adhoc networks. Several technician and specialist are working on the success of these techniques which can eventually uphold the security and authenticity of the information among MANETS especially in the field of military services.

Conclusion

This paper comprehensively tackles the identity-based cryptography and how it is utilized in securing the mobile ad hoc networks in the information technology. Though the IBC had proven to be an efficient mechanism of securing and keeping safe confidential information, still it has its limitations that must be addressed properly in order to ensure efficiency and proficiency of its functions.

Works Cited

Balfe, Shane., Boklan, Kent., Klagsbrun, Zev and Paterson, Kenneth. “ Key Refreshing in Identity-Based Cryptography and its Applications in MANETS” (2007). University of London. 1-8. Accessed 27 November 2014.

Pura, Mihai and Buchs, Didier. “A Self-Organized Key Management Scheme for Ad Hoc Networks Based on Identity-Based Cryptography”. (2014). Military Technical Academy. 1-4. Accessed 27 November 2014.

Sagheer, Ali and Taher, Hadeel. “Identity Based Cryptography for Secure AODV Routing Protocol”. (2012). 198-201. Telecommunications Forum. Accessed. 27 November 2014.

Youngblood, Carl. “An Introduction to Identity-based Cryptography”. (2005). CSEP. 1-7. Accessed 27 November 2014.