Identity Based Cryptography A Technical Review

Mohammed A. Khasawneh
Concordia Institute for Information Systems Engineering
Concordia University
Canada, Montreal
moh_kh86@yahoo.ca

Ammar Abdallah
Software and IT Engineering, École de Technologie Supérieure
University of Québec
Canada Montréal
ammar.abdallah.1@ens.etsmtl.ca

Abstract

This Paper aims to have a comprehensive discussion on identity-based cryptography and aims to have a detail explanation on its technical aspect. Moreover, it discusses on how IBC helped in securing the confidentiality and authenticity of messages in 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 and on the development of new techniques that can strengthen the security and protection of the messaging system in the area of wireless communication.

Keywords: ad hoc network, identity-based cryptography, information technology

1. 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 et al (2014). 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 A. M. Qadir et al (2019).

1. Concept of identity-based cryptography

Cryptography is a science and art of message encryption that transforms a message into a covered version that cannot be intercepted and understood by unauthorized individuals, but it can be successfully received and understood by the anticipated receiver. The procedure of encrypting and decrypting a message is governed by keys which are commonly composed of the small information and cryptographic algorithms Pura et al (2014). It is used in order to provide security goals among ad hoc networks especially that the lots of threats are experienced in this communication system.

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 et al (2014). Both the public and private keys are interrelated in the sense that only the public key which is utilized in encrypting messages and on the other hand it is the matching private key which can be employed in decrypting the code. Therefore, if an outsider compromises the public key, it is them not viable to figure out the private key, hence the message will not be decoded. The relevance of identity-based cryptography is that it requires accurate validation of certificate since it involves multiple node certificate instead of a chain of certificates W. Ao et al (2019).

The procedure of encryption indeed ascertains the confidentiality of the message that is sent. It is accompanied by having a digital signature that strengthens the security goals of the message. The transmission of the message is done by sending a message using the algorithm key and a private key as signature of the message. Then the message along with the signature is sent to the receiver, and the recipient will also apply the verification algorithm on the message-signature pair. This verification algorithm needs a verification key which is the public key provided by the signer in order to verify the documents or messages. It is after the verification stage wherein the message will be accepted or rejected depending on the result of the verification. The figure 1 shows how the encryption and decryption occur.

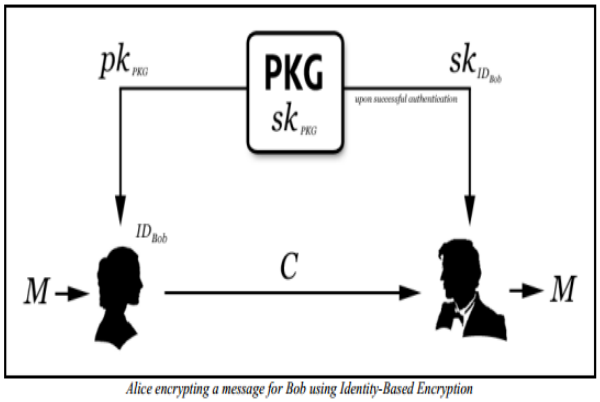

Figure 1. The encryption and decryption process (Youngblood, 2).

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.

2. Application of the identity-based cryptography in the ad hoc and MANET:

Mobile ad hoc network is one of the commonly discussed and researched in the area of wireless communications because unlike the conventional communication networks it requires no access point or node. It is a network which is composed of only the mobile devices like a personal digital assistant or even a laptop. MANET needs no centralized infrastructure or wireless routers but it only operates using nodes that are connected to each other through the ad hoc model hence this system is more dynamic as compared to the usual communication networks The network is temporary because it does not depend on existing infrastructure, such as routers in wired networks or access points in managed wireless networks (infrastructure).

MANET is equipped with several security countermeasures. It does not have the pre-existing infrastructure or the conventional system topology therefore the data is transmitted through the nodes in a multi-hop manner. Energy sources of MANET device is limited, especially the life of its transmitting range therefore its physical security is relatively poorer. This simply means that the MANET devices can be easily accessed and stolen, and the physical signal are prone to spoofing and hacking. Hence, the management of the mobile ad hoc network is enhanced mainly on the key management and the routing security Manohari et al (2016).

At present, several proposals that aim to protect the potential security threats started on the identification of the security threats and then after this stage they have find an appropriate solution to the observed problem. An example of a solution proposed is by enhancing the existing protocol in order to prevent the possibility of being hacked. Some have even proposed better and newer schemes to increase the security of the system.

Various security countermeasures have been utilized through the use of cryptography technologies. One of which is the identity-based cryptography which is utilized in the mobile ad hoc networks. This technique is classified into two categories- the symmetric key-based and the asymmetric key-based Sagheer et al (2014). These two categories differ on their dependence on the availability and security of the Certificate of Authority.

In the symmetric cryptography, if a hacker figured out the symmetric key of the group users all the encrypted messages for the group will be revealed. However, the asymmetric system even if the users public key is being intercepted; it does not affect the public keys of the other users. The AC rely on the public key infrastructure (PKI) which requires a control point which is proven to be trusted, hence it is more expensive than the symmetric cryptography. However, t is important to know that the technology in the asymmetric cryptography is very much dependent on the availability and security of a Certificate Authority S. Xu and T. Saadawi (2001).

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 et al (2014). This ad hoc network operates through a secured and protected network 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 Tanweer Alam (2019).

In figure 2 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).

Figure 2. Typical Architecture Diagram for Mobile Ad-hoc Network (MANET)

Balfe et al (2014) 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 connection within the network, as long as the nodes communicate then the exchanging of messages can be 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 Alam et al (2018).

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 Sagheer et al (2014).

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 et al (2014).

3. 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 et al (2014). The research and development of the mobile ad hoc network security is still on its early stage, hence diverse security plans have been proposed and utilized and have been proven to be effective in wired network communication however, there was no single device that provides all the required services in MANET. Because of it's some certain protection mechanism, not all communication mechanisms are applicable to it. Youngblood (4) enumerated these special mechanisms as follows: a) lack of network infrastructure

and online administration; b) forceful of network topology and node membership; c) potential threats from the inside the network; and d) the possibility of ACM transactions on computational logic.

One great 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) Sagheer et al (2014) 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.

Another major predicament experienced in public-key based security system is that there is the need for every public key of the users to be available for other users in order to verify its legitimacy. This is a great problem in mobile ad hoc network system especially that there are no centralized services and there is no presence of possible network partitions (Youngblood, 5). Another issue that must be resolved in the IBC utilization of MANET is the trust distribution that occurs during the sharing of the keys and secret codes among node users. A great deal of trust or secret for the management of the keys should be observed in distributing the keys internationally or regionally. Moreover, the cooperation distribution can also be a cause of inefficiency and susceptibility for the security attacks among ad hoc network systems Yu et al (2019).

Aside from securing the safety and confidentiality of the messages through the mobile ad-hoc 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 ad-hoc 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 M. Sharma et al (2019).

The security attacks have been observed to be rampant in the field of information technology in these modern days despite the extensive use of identity-based cryptography. These security aggressions have been found out to cause trouble and can compromise the validity and confidentiality of the information and messages send through the ad hoc network system. Further, information terrorism may alter, release or deny data. Hence, it is the goal of the experts to secure the data. In strengthening the data safety, a security protocol must be established, and this must uphold the safety attributes of data such as privacy, accessibility, reliability, legitimacy and no repudiation Balfe et al (2014).
In order to prevent the case of hacking and intercepting messages, a new scheme that surely preserves the communication security is being administered (Youngblood, 6). This is done by having all network operations in trust phase among all nodes in a secure environment. During its implementation, every communication device in the ad hoc network identifies the sensing node of its neighboring devices and provides them with its public keys. This is actually the public key sharing process to the neighboring nodes. When public key transfers are done, each node is given certificates of authenticity in an encrypted form. This makes the node secured and free from intruders and hackers.

4. 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 in securing and keeping safe of confidential information, still it has its limitations that must be addressed properly in order to ensure efficiency and proficiency of its functions.

The paper further cited some of the related works and advancement in the area of wireless communication that promotes more secured and protected transmission of messages. These new schemes can be utilized as bases for administering programs and security plans in the promulgation of confidentiality, availability and authenticity of messages.

Reference

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.

W. Ao, S. Fu, C. Zhang, Y. Huang and F. Xia, "A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography," 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 2019, pp. 90-95, doi: 10.1109/CCET48361.2019.8989361.

Manohari, P.K., Ray, N.: Multipath routing protocols in MANETs: A Study. In: (ICICCS), pp. 91–96 (2016).

Alam T, Benaida M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84. DOI: https://doi.org/10.3991/ijim.v12i6.6776.

Tanweer Alam, “Blockchain and its Role in the Internet of Things (IoT)”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 151-157, 2019. DOI: https://doi.org/10.32628/CSEIT195137.

Yu, Sui, Lichen Zhang, Lixia Li, Bin Yan, Zhipeng Cai, and Lizong Zhang. "An Efficient Interest-aware Data Dissemination Approach in Opportunistic Networks." Procedia Computer Science 147 (2019): 394- 399.

M. Sharma, M. Singh, K. Walia and K. Kaur, "Comprehensive Study of Routing Protocols in Adhoc Network: MANET," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 0792-0798, doi: 10.1109/IEMCON.2019.8936135.

S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks," in IEEE Communications Magazine, vol. 39, no. 6, pp. 130-137, June 2001, doi: 10.1109/35.925681.

A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757514.

Biographies:

Mohammed A. Khasawneh received his master's degree in Information and system Engineering from Concordia University, Canada and bachelor's degree in Computer Science from Jordan University of Science & Technology (JUST), Jordan. He is currently pursuing his PhD in Information and system Engineering in Concordia University, Canada. His current research interests include Intelligent Transportation System, machine learning and artificial intelligence.

Ammar Abdallah Qasaimeh is a doctoral researcher in Software Engineering and Information Technology and a web analytics professional. He received his PhD from École de technologies supérieure (ETS) University of Québec (Montreal, Canada) in 2019, his Master's degree in quality systems engineering from Concordia University (Montreal, Canada) in 2014 and his Bachelor's degree in computer science from Al-Balqa Applied University (Jordan) in 2011. His research interests are not limited to but include enterprise architecture, software engineering measurement and standards, web analytics, and agile methodologies.