Survey on Key Management Schemes for Constraint Environment of WSN

Kumail Lakhani
Dept. of Electronics and Telecommunication Engineering
DJ Sanghvi College of Engineering,
University of Mumbai

Ashwin Nivangune
CDAC, Mumbai

T. D. Biradar
Dept. of Electronics and Telecommunication Engineering
DJ Sanghvi College of Engineering,
University of Mumbai

ABSTRACT

Wireless Sensor Networks (WSN) is becoming the heart of many applications. Data integrity and security is a major issue as the wireless sensor nodes are exposed to harsh and hostile environment. This paper highlights the merits and demerits of different key management schemes under the broader classification of Public Key Infrastructure (PKI), Identity Based Encryption (IBE) and Certificateless Signcryption. These schemes will provide authentication and thereby secure the communication between the nodes considering the constraint environment of the wireless sensor network. Selection of these key management schemes depends upon the application specifications, functionality and computational complexity.

Keywords

WSN, key management schemes, PKI, IBE, Certificateless Signcryption, security, data integrity

1. INTRODUCTION

With the recent advancement in technology, wireless sensor networks find its applications in many areas, such as military defense systems, medical health care systems, industrial sector, Internet of things (IOT), etc. The basic task of the sensor motes is to gather information, perform processing and forward it to the desired destination. Also, wireless sensor motes have a limited computational capacity, and battery life. Considering these constraints, symmetric cryptography was adopted which utilized nominal amount of energy for computation and communication. However, it proved to be insecure to quiet an ex- tent, as the symmetric key generated for communication could not be shared with the respective nodes in a secure manner. In order to address this problem the concept of public key cryptography (PKC) was coined. PKC defines key pairs (public & private keys) for encryption and decryption. Hence there was no need to share any key between the communicating nodes; however it burdened the computational complexity. In order to avoid the nodes being compromised, there was a need of a key management scheme which would provide confidentiality, data integrity, along with authentication and Non-repudiation. Simultaneously the wireless constraints necessitated the need to design energy efficient key management schemes. Over the years different key management schemes were proposed which can be basically classified into 3 types as shown in Fig 1 ,

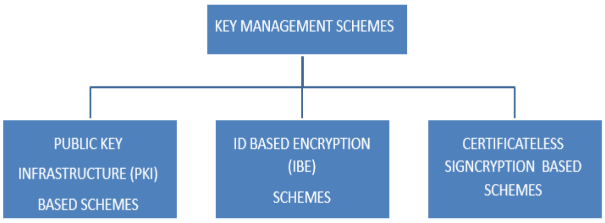
KEY MANAGEMENT SCHEMES
PUBLIC KEY INFRASTRUCTURE (PKI) BASED SCHEMES
ID BASED ENCRYPTION (IBE) SCHEMES
CERTIFICATELESS SIGNCRYPTION BASED SCHEMES

Fig. 1: Classification of Key Management Schemes

The footprint of the paper is organized as follows: Section 2 gives detailed overview of classification of various PKI based key management schemes. In section 3 and section 4 we have discussed key management schemes based on IBE and Certificateless signcryption schemes respectively. We conclude in section 5 by analyzing an efficient scheme as per the wireless sensor network constraints.

2. PUBLIC KEY INFRASTRUCTURE (PKI) BASED SCHEMES

Public key infrastructure (PKI) is a well-known architecture used for key management. PKI architecture is used to generate an authentication between two end users using digital certificates where a trusted third party is used in the authentication process called the certifying authority (CA). The digital certificate is used to associate an individual’s identity with its corresponding public key which is cross verified by the trusted third party (CA). In doing so it primarily requires the user’s credentials to be sent to the Registration authority (RA) who is responsible for verification. Later the CA sign and returns the digital certificate to the respective user.

The authentication part is explained as follows; let us assume that Bob (sender) wants to establish communication with Alice (receiver).Thus he acquires the digital certificate of Alice and verifies whether the certificate was issued by the trusted CA. Here it is assumed that the Public key of the C.A and the digital certificates are globally known to everyone. The Certificate Verification process can be clearly understood from the following Fig 2.

From the diagram it’s understood that when the comparison of the hash of publicly available information and the result of the decryption of the signature with the public key of the CA are same then the certificate is authentic.

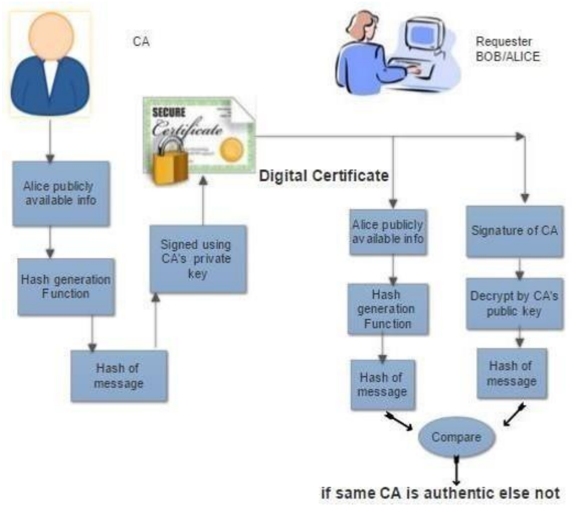

Fig. 2: Digital Certificate Verification

The following Fig 3 explains communication establishment procedure between Bob and Alice.

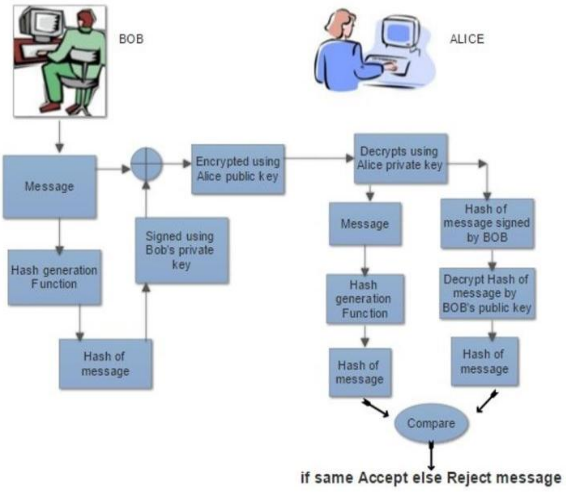
BOB
ALICE
Message
Hash generation Function
Hash of message
Signed using Bob's private key
Encrypted using Alice public key
Decrypts using Alice private key
Message
Hash generation Function
Hash of message
Hash of message signed by BOB
Decrypt Hash of message by BOB's public key
Hash of message
Compare
if same Accept else Reject message

Fig. 3: Communication between Bob and Alice

It is observed that only when both the hash values are equal Alice is assured that the It is observed that only when both the hash values are equal Alice is assured that the message is sent by Bob, and she accepts the message. In the following part of this section we discuss the various proposed PKI based schemes.

2.1 Lightweight PKI for WSN micro-PKI:

This scheme was introduced by B. Kadri et al in 2010 [1] which utilized a lighter version of the PKI model that can be implemented on a wireless sensor network considering the energy constraints. Here the digital certificate was replaced with a random key which would be generated by each node and stored by the CA. If any node in the network wants to establish communication with each other than on the basis of the request made the CA would establish its own session key and encrypt it with their respective random keys. The nodes can then use that session key as a symmetric key for further communication, giving the system a certain level of data integrity and authentication.

2.2 PKC based approach for securing SCADA communications:

In this paper A. Saxena et al in 2012 [2] proposed a scheme based on the PKI model for SCADA communication. This scheme works with an assumption that the digital certificates are not globally known and have to be requested from the CA. Moreover to make the scheme more energy efficient the digital certificates were replaced with the MAC address of each node. The verification process was done on the basis of the MAC addresses of the respective nodes. This scheme also proposes an efficient way for multicasting and broadcasting.

2.3 Simple Secure PKI-based Scheme for Wireless Sensor Networks

In 2011 Omar Alfandi et al [3] proposed scheme which utilizes PKI architecture during the handshake process to generate 128 bits symmetric key. In this scheme, Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) are used for digital signature generation and encryption respectively, whereas Hash calculation and verification is done using HMAC. XTEA is used for symmetric encryption. The advantage of this scheme over the previous schemes was that along with authentication and data integrity it was also able to detect replay attacks, as both the nodes who wanted to communicate had to actively generate the symmetric key. In 2013 Omar alfandi [4] made a brief study of different encryption, decryption hashing and digital signature algorithms and concluded that the scheme which he defined previously can be enhanced by replacing XTEA by AES-128, and HMAC by CCM or CMAC.

2.4 Efficient and Scalable Public Key Infrastructure for Wireless Sensor Networks

In 2015 Daehee Kim [5] proposed a remarkable scheme using PKI for a wireless sensor network. He proposed an energy efficient system by using a hierarchical structure where the nodes used at the top of the hierarchy were termed as High sensor nodes (HSN) which had greater battery life and increased computational capacity and the bottom nodes were known as low sensor node (LSN). The system was designed in such a way that maximum computation was done by the HSN leaving no burden on the LSN, hence it thereby made the system energy efficiency. Also, this scheme enhances the security of the system by distributing the polynomial share of the CA's private key amongst the 'n' number of HSN's. The security of the scheme is based on the (k,n) threshold scheme where 'n' is number of HSN having the polynomial share of the private key and 'k' represents the total number of polynomial share required to generate the complete private key. Hence until the 'k' number of HSN's are not compromised the system remains secure. The energy efficiency can be enhanced by making use of Elliptic curves for digital signatures and encryption. The drawback of this scheme is that HSN are quite expensive as compared to LSN, however the scheme utilizes more number of LSN due to which the overall cost does not increase drastically.

3. ID BASED ENCRYPTION (IBE) SCHEMES

Identity based encryption is an alternative to PKI, which was proposed by Shamir in 1984. The ideology behind this scheme was to overcome the problem of generation and management of certificates by the certifying authority (CA), which will thereby reduce the system complexity. The basic idea behind IBE was to replace the public key associated with the digital certificate by an identity (ID) of an individual which will act as the public key. The identity of the individual could be any string value (email ID, Phone number, etc.) related to that individual.

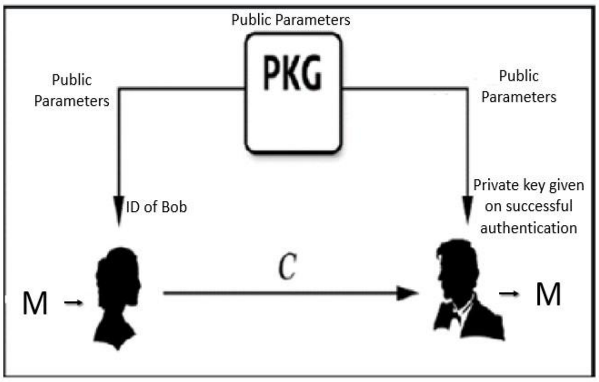

Fig. 4: Schematic outline of an IBE communication Scheme [6]

From the following Fig 4 we analyze the implementation of an IBE system. Initially a private key generator (PKG) is created, which consist of the master key. This is analogous to a CA in PKI. The PKG gives out public parameters, which is used along with the ID (public key) of the receiver to encrypt the given data and sent. At the receiving end the receiver first has to authenticate its identity (ID) with the PKG, post which the PKG gives out a private key for the corresponding identity (ID) if authenticated. Upon receiving the private key and public parameters from PKG the receiver decrypts the cipher text to obtain the plain text.

The different kind of ID based encryption schemes proposed are discussed below:

3.1 Identity-Based Encryption from the Weil Pairing:

On the basis of the IBE concept proposed by Shamir, D.Boneh and M.Franklin in 2001 [7] was the first to propose a fully functional identity-based encryption scheme for a chosen cipher text attack using the random oracle model. This scheme uses Weil pairing based on bi- linearity as the main algorithm used for the construction of the scheme. This paper explains the implementation in two parts where initially they explain the BasicIdent model which is secure against chosen cipher text attacks which is eventually converted to a FullIdent model as it is secure against adaptive chosen cipher text attacks. The security of this system is based on the assumption of Die-Hellman for elliptic curves.

3.2 Secure Identity based Encryption without Random Oracles:

In 2004 D. Boneh and X. Boyen [8] proposed a proof for a completely secure IBE system without the random oracle model. Prior to this, efforts were taken by canettie et al in 2003 to successfully develop a selective ID based scheme without random oracles with weaker security. Here the adversary has to commit to the ID it chooses to attack before time. In order to overcome this drawback in security Boneh and Boyen constructed a security model based on the decisional bilinear Diffie-Hellman assumption, due to which the security of the system improved with a polynomial time reduction. The major disadvantage of the system is that this scheme can be practically realized only for a selective ID based construction.

3.3 Hierarchical Identity Based Encryption (HIBE) with Constant Size Ciphertext

The concept of Hierarchical IBE was introduced by C.gentry and A. Silverberg [9] in 2002 using the BDH assumption in the random oracle model. The vision behind proposing a HIBE scheme was to reduce the responsibility of the PKG where the root PKG generates private keys for subordinate PKG's and later it issues this private key for the end users. This would prove to be efficient in a big network with many users. Later in 2004 Boneh and Boyen [8] proposed a selective ID secure HIBE without random oracles. The drawback of this scheme was that the length of the cipher text and private key grows linearly with an increase in the hierarchy depth. In order to overcome this drawback Boneh Boyen and Goh [10] constructed an IBE scheme where the length of the cipher text was independent of the depth of the hierarchy. However the length of the private key decreases with increase in hierarchical depth, which restricts the number of hierarchical levels to a certain limit. The security of this scheme is based on the bilinear diffie-hellman inversion assumption. This scheme provides security against selective ID attacks, and observes an exponential degradation in a full security model (with or without random oracles).

3.4 Practical Identity-Based Encryption without Random Oracles

The work done by Craig Gentry [11] in 2006 overcame the problems faced previously, as he was able to define a practical IBE construction with shorter public parameter. In the standard model (without random oracles). The security of this scheme works with an assumption of the private key queries made by the adversary and obtains a tighter reduction based on the q-ABDHE decision assumption, where q is the anticipated number of queries. The only problem with this scheme is that the assumption used was relatively very large for the construction; moreover the assumption was not as satisfying as it is dependent on 'q' and not concrete.

3.5 Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions

The milestone achieved by Brent waters [12] in 2009 was remarkable as he introduced the concept of dual system encryption, which gave proof of full security in the standard model. The advantage it gained over Gentrys [11] scheme is that the assumption he used was relatively small and simple. The security of this scheme is based on decisional Bilinear Die-Hellman and decisional linear assumptions. In the construction part he introduced the concept of semi-functional private keys and semi- functional cipher text, to be used with normal private keys and ciphertext which enhanced the security of his construction with simpler assumptions. In the work presented he has also extended his security proof to the HIBE system and have established full security for a HIBE construction with smaller assumptions.

4. CERTIFICATELESS SIGNCRYPTION SCHEMES

The generation of ID based cryptography was able to overcome the biggest drawback of certificate generation and management over PKI but it did not provide key escrow, as the PKI architecture did. The reason being is that the private key generated using ID based cryptography was a combination of 2 partial secrets, one coming from the PKG and the other coming from the user. In order to overcome this issue Al- Ryiami and Paterson [13] in 2003 proposed the concept of certificateless singncryption which took the advantages of both ID based cryptography and PKI. In doing so, authentication and integrity was taken care of without using digital certificates along with the property of key escrow.

In the following part of we have described different certificateless signcryption schemes which was proposed followed by their advantages and disadvantages.

4.1 Certificateless Signcryption schemes with bilinear pairing

After the introduction of this concept a lot of research work was done on bilinear pairing which proved to be impractical due to the costing and computational length of the key pairs. Barbosa and Farshim [14] in 2008 proposed a certificateless signcryption scheme which was provably secure using random oracles. Later, W. Xie and Z. Zhang [15] in 2009 proposed a new certificateless signcryption schemes with their security proofs using the random oracle model, but in 2010 Selvi et al [16] proved that these schemes are insecure against type 1 adversary attacks.

Z.H. Liu [17] in 2010 proposed a certificateless signcryption scheme in the standard model where he gives proof of his scheme being efficient and practical. How- ever, in 2011 J. Weng[18] proved that the scheme pro- posed by Liu et al is insecure under type-2 adversary at- tacks. Thereafter efforts were taken by many researchers to address the above issue but it did not proved to be successful. In order to overcome all these previous drawbacks a remarkable milestone was achieved by Hongzhen Du [19] in 2016.He proposed an efficient certificateless signcryption scheme which is secured using random oracles and where message confidentiality, signature unforgability, public verifiability and forward secrecy are taken care of. Moreover this scheme also achieves smaller ciphertext size and hence could be used with smaller bandwidth.

4.2 Certificateless Signcryption schemes without bilinear paring:

Along with approaches developed on certificateless signcryption using bilinear pairing, attempts were also made to achieve security without using bilinear pairing. Some schemes were also proposed without bilinear pairing using random oracles, but were found to be impractical. Attempts were made further on to achieve security, but till date full security proof for a certificateless signcryption scheme without bilinear pairing is still an open problem

5. CONCLUSION

In this paper, we survey the state of the art of different key management schemes and have discussed the advantages and disadvantages of each scheme in detail. Certificateless signcryption with bilinear pairing scheme stands apart as it combines the merits of both PKI and ID based encryption schemes. Moreover the scheme proposed by Hongzhen Du also provides reduced ciphertext size, and reduced computational complexity. Hence we conclude that certificateless signcryption based schemes could be used to secure a wireless sensor network considering its constraints.

6. REFERENCES

[1] B. Kadri, M. Feham, and M. Abdallah, “Lightweight1 PKI for WSN PKI,” vol. 10, no. 2, pp. 135–141, 2010.

[2] A. Saxena and Z. Saquib, “PKC based approach for securing SCADA communications,” vol. 3.

[3] O. Alfandi, A. Bochem, A. Kellner, and D. Hogrefe, “Simple Secure PKI-based Scheme for Wireless Sensor Networks,” pp. 359–364, 2011.

[4] “Improving energy efficiency of data communication in a hybrid PKI-based approach for WSNs,” *2013 IEEE 10th Consumer Communications and Networking Conference, CCNC 2013*, pp. 697–700, 2013.

[5] D. Kim, S. Member, and S. An, “Efficient and Scalable Public Key Infrastructure for Wireless Sensor Networks,” no. 2012, 2014.

[6] H. D. Phaneendra, “Identity-Based Cryptography and Comparison with traditional Public key Encryption: A Survey,” *International Journal of Computer Science and Information Technologies*, vol. 5, no. 4, pp. 5521–5525, 2014.

[7] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[8] D. Boneh and X. Boyen, “Secure Identity Based Encryption without Random Oracles,” *Crypto*, pp. 443–459, 2004.

[9] C. Gentry and A. Silverberg, “Hierarchical ID-Based Cryptography,” Advancesin CryptologyASIACRYPT 2002, vol. 2501, no. 2002/056, pp. 548–566, 2002.[Online].Available:http://www.springerlink.com/index/vmbyu grnkymnc965.pdfhttp://link.springer.com/10.1007/3- 540 36178-2_34

[10] D. Boneh, X. Boyen, and E.-j. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Advances in Cryptology EUROCRYPT 2005, Springer, 2005., vol. 3493, no. Lecture Notes in Computer Science, pp. 440–456, 2005.

[11] C. Gentry, “Practical Identity-Based Encryption Without Random Oracles,” Eurocrypt, vol. 4004, pp. 445–464, 2006.

[12] B. Waters, “Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in informatics), vol. 5677 LNCS, no. 2006, pp. 619–636, 2009.

[13] S. Al-Riyami and K. Paterson, “Certificateless public key cryptography,” Advances in Cryptology-ASIACRYPT 2003, pp. 452–473, 2003.[Online]. Available: http://link.springer.com/chapter/10.1007/978-3-540-40061529\nhttp://www.springerlink.com/index/4wc47elk 7fp8xw ty.pdf

[14] M. Barbosa and P. Farshim, “Certificateless Signcryption,” ACM symposium on Information, computer and communications security, pp. 369– 372, 2008.

[15] W. Xie and Z. Zhang, "Efficient and Provably Secure Certificateless Signcryption from Bilinear Maps *," pp. 1–21.

[16] S. D. Selvi, S. Vivek, and C. Rangan, "Security Weaknesses in Two Certificateless Signcryption Schemes," pp. 1–3, 2010. [Online]. Available: http://eprint.iacr.org/2010/092

[17] Z. Liu,Y.Hu,X. Zhang, and H.Ma, "Certificateless signcryption scheme in the standard model," Information Sciences, vol. 180, no. 3, pp. 452–464, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2009.10.011

[18] J. Weng, G. Yao, R. H. Deng, M. R. Chen, and X. Li, "Cryptanalysis of a certificateless signcryption scheme in the standard model," Information Sciences, vol. 181, no. 3, pp. 661–667, 2011. [Online].Available: http://dx.doi.org/10.1016/j.ins.2010.09.037

[19] H. Du, "Efficient Certificateless Signcryption from Bilinear Pairings," vol. 10, no. 4, pp. 303–316, 2016