IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

A Survey of the Various Identity-based Encryption Techniques in Wireless Sensor Networks

Shrishty Gautam[1], Charu Wahi[2], Seema Sharma[3]

M.Tech Student, Birla Institute of Technology, Mesra, Ranchi, India[1]

Assistant Professor, Birla Institute of Technology, Mesra, Ranchi, India[2, 3]

Abstract: Identity Based Encryption (IBE) is an encryption technique that was developed, keeping in mind, the wireless sensor networks. IBE is an encryption mechanism that makes use of the user's identity, such as, e-mail ID, phone number, date of birth, or their combination as the key. IBE was developed for cases where pre-distribution of the public key was infeasible or not possible due to certain technical issues. Thus, using IBE, encryption can be performed, without the recipients public key. In this paper, we survey the various Identity based encryption techniques that have been proposed till now. We present a comparative analysis of the work done till now. We also provide a view on the relative advantages and drawbacks of the provided schemes. We also give a look into the futuristic scope of IBE online/offline encryption systems. These algorithms have been proposed and are currently being widely used in Wireless Sensor Networks. We provide an overview of why IBE is highly secure and suitable to WSN.

Keywords: Identity Based Encryption (IBE), Random Oracle, Diffie-Hellman Assumption, Bilinear Diffie-Hellman Assumption (BDH), Decision Bilinear Diffie-Hellman Assumption (DBDH), Decision Bilinear Diffie-Hellman Inversion Assumption (DBDHI), Public Key Generator (PKG).

I. INTRODUCTION

Wireless Sensor Networks, sometimes called as Wireless Sensor and Actuator Networks (WSAN) are spatially distributed autonomous sensors that monitor physical or environmental conditions for example temperature, pressure etc. and pass that data through the network to a main location. It consists of several hundreds or thousands of nodes that are connected to one or more sensors called as the Base Station. Sensors are usually small in size and can store a small amount of information. Sensors include a radio transmitter with an antenna, a microcontroller, an interfacing electronic circuit and a power source like a battery. They were initially proposed and developed for military use, carrying sensitive data. But now they are also being employed in other fields like health, architecture, oceanic monitoring, earthquake monitoring etc. A major advantage of WSN is that they perform data processing within the network so that large streams of data need not be aggregated into the system. Hence, since the nature of the information carried is highly sensitive, it becomes imperative to make the system secure. However, security in WSN systems comes with its own challenges.

WSN systems are prone to a variety of attacks that includes node tampering, node capture, denial of service attacks etc. there are five main challenges associated with security:

i. The nature of communication: Wireless
ii. The sensor nodes are limited in terms of resource
iii. If the WSN is very large or dense
iv. There is a lack of fixed infrastructure
v. Prior to deployment, the network topology is unknown

Hence, we require strong and efficient key distribution mechanisms. The existing cryptographic mechanisms depend on a single key that is distributed among each node. This method is highly inconvenient and consumes a lot of storage space. It causes processing overheads since the nodes can only store a small amount of information and the key sizes that are used in typical cryptosystems is too large. Also since, the key is being shared among various nodes, there is a high chance of the key being intercepted easily by an outside attacker. As a result, there needs to be a more efficient way to provide security within the network. Shamir [1] proposed the concept of Identity based Encryption and Identity Based Signature schemes in the year 1984.

In the following sections, we would study about Identity Based Encryption (IBE). We would also compare the various IBE based proposed systems, in terms of their advantages, disadvantages and proposed applications.

II. IDENTITY BASED ENCRYPTION

A.Shamir [1] proposed the idea of Identity Based Cryptosystems in 1984. IBE is a primitive of Identity Based Cryptosystems. IBE is a public key encryption mechanism which makes use of any plaintext that provides a valid identity for the user, as its key. For example, the userse-mail address, phone number, date of birth, or may

DOI 10.17148/IJARCCE.2017.6163

be a combination of these can be used as a valid public key. Through Identitybased systems, anyone can generate a key. A Private Key Generator (PKG) is used for the generation of private key. Basically, the PKG first generates a Master Public Key and publishes it to the network. Now, any party that wants to communicate can generate a public key by combining the Master Public Key with the identity (ID) of the user. For the corresponding Private Key, the authorized user contacts the PKG.The PKG then uses the Master Private Key also called as the Master Key, which it retains, to generate the Private Key. Thus, IBE does not require any mechanism for public key distribution, hence eliminating the need for a Public Key Infrastructure. However, the PKG used to decrypt the messages needs to be extremely trusted and secure, as, it has the capability of generating the private key for anyone. One of the main problems IBE faces here is Key Escrow which is inherent in the system. Key Escrow is "an arrangementin which the keys needed to decrypt encrypted data are held in escrow, so that, under certain circumstances, a third party may gain access to the keys." [14]There have been various systems proposed to overcome this problem we will read about them in detail in the sections below.

A. Protocol framework

There are 4 basic algorithm that form the framework of IBE systems.

- **Setup:** This algorithm is run only once by PKG. It takes as input a security parameter and outputs the message space and the ciphertext collectively called as P along with the master key
- **Extract:** It is run when the private key is requested. It takes P, master keyand ID as input and outputs private key.
- **Encryption:** Takes P, a message and ID as input and encrypts it to give cipher text.
- **Decryption:** Takes private key, P and cipher text as input to give the original message as the output.

B. Advantages:

- Eliminates the requirement of a Public Key Infrastructure.
- It guarantees Authenticity of the user and provides Confidentiality of the message and Integrity.
- Allows the messages to be time-stamped so that, if a message arrives out of time, to avoid duplicity, the system can render it expired.
- As the users own identity is used for key generation, no additional certificates are required.
- For future decryption, it allows the messages to be post-dated.

C. Disadvantages:

- Since the PKG keeps a track of all the Pubic-Private key pairs, if it is compromised, then the entire system becomes compromised. Hence, the PKG needs to be highly secured.
- As the PKG has the ability to generate private keys whenever it requires, it can decrypt the messages even without user authority. In such a case, the user can altogether deny the authencity of the data sent. Hence, it leads to Repudiation.
- Since it requires a centralized server, many keys are held in escrow and can be easily exposed. Hence, t is not free from Key Escrow.
- A secure channel of transmission is required between sender/receiver and the IBE server.
- IBE solutions aren't immune against code breaking Quantum computer attacks.

III. VARIOUS IBE SCHEMES

We now go through the various IBE based schemes proposed by eminent researchers. We look at the basic system that was proposed and how it works for the WSN environment.

A. Identity based cryptosystems and signature schemes:

A. Shamir [1], in 1984, proposed a new Identity based cryptosystem. Through this system, any number of users could communicate securely with each other, without having to exchange any public key or private key and without the need of a third party. In this scheme, the user would use his own name and address or social security number, or any form of personalized identity to create his very own key, instead of the random, system generated public-private key pair. This method eliminated the need for digital certificates, which can sometimes be tedious. Hence, the proposed system reduced complexities and cost of establishment for the PKI.

Shamir [1] based his system on RSA algorithm and Integer Factorization Problem. However, he could only implement Identity Based Signature scheme and not Identity Based Encryption. In ID based signature scheme, the digital signatures could be verified using information about the user that was publicly available, such as user's identity. The problem that Shamir [1] faced while implementing IBE was that, he was unable to come up with a practical solution for acquiring the public key before encryption.This became an "open problem" which was resolved in 2001 by Boneh and Franklin [2].

The proposed system was implemented in the form of smart cards and required the users to be aware and careful of their smart cards being misusedwhich became a problem, as, if a user loses his smart card, it can be used by anyone who finds it.

B. Identity based encryption from weil pairing:

In 2001, Dan Boneh and Matthew Franklin[2], proposed a fully functional Identity Based Encryption scheme which solved Shamir's problem. The systems security was based on the Bilinear Diffie-Hellman Assumption using Random Oracle and Bilinear Non-Degenerate Maps.

Bilinear Diffie-Hellman Assumption "is a computational hardness assumption about a certain problem involving

DOI 10.17148/IJARCCE.2017.6163

discrete logarithms in cyclic groups.” [14] It is used in many cryptographic algorithms to prove the security.
Random Oracle is an “oracle (theoretical black box) that responds to every unique query with a unique query with a (truly) random response chosen uniformly from its output domain.” [14].It is basically a “Mathematical function, which maps each query to a random response from its output domain”. For any repeated queries, it gives back the same output as before. Weil Pairing curves [14] were used to implement the assumption.

Bilinear Non-Degenerate Maps: Let G1 and G2 be two groups of order q for some large prime q.(The proposed IBE system makes use of a bilinear map ˆ e : G1 × G1 → G2 between these two groups. The map must satisfy the following properties:
1. Bilinear: We say that a map ˆ e : G1 × G1 → G2 is bilinear if ˆ e(aP,bQ) = ˆ e(P,Q)ab for all P,Q ∈ G1 and all a,b∈ Z.
2. Non-degenerate: The map does not send all pairs in G1 × G1 to the identity in G2.
Observe that since G1,G2 are groups of prime order this implies that if P is a generator of G1 then ˆ e(P,P) is a generator of G2. G1 is an additive group of points along an elliptic curve. G2 is a multiplicative group of point along a finite field of points.
3. Computable: There is an efficient algorithm to compute ˆ e(P,Q) for any P,Q ∈ G1.
A bilinear map satisfying the three properties above is said to be an admissible bilinear map. The Weil pairing can be used to construct an admissible bilinear map between these two groups.
In this system, even if the attacker obtains several private keys, without the corresponding ID, they cannot attack the message even if they themselves choose the data to be attacked. Hence, this scheme is CCA secure i.e. Chosen Cipher-text Attack.
This scheme does not require the receiver to make any preparations for receiving the message. The PKI is maintenance free. This scheme can also work with signatures and has a highly secured PKG. Since the PKG is distributed over the network, the Master Key is never available in just one place, hence, making it more secure and robust.
Along with advantages, there are also certain drawbacks. The system gives a higher preference to private key holding, hence the user needs more assurance from the system, and also the PKI availability needs to be high. Another drawback is that, the system depends on key escrow especially during decryption and the signature verification. This means that these steps occur in the server where, a third party is responsible for the maintenance of the keys and under circumstances, it can make the private keys available to a third party authority.

C. Selective id secure identity based encryption without random oracles:

Dan Boneh and Xavier Boyen[3], in the year 2004, proposed a Hierarchical Identity Based Cryptosystem, which did not use Random Oracles.Boneh, Boyen along with Ghuo [4] in 2005 also proposed a Hierarchical IBE which was an improvement on the previous Boneh-Franklin [2] model. They proposed two IBE systems, both Selective Identity secure, where the user chooses in advance, the identity to attack. This was however, less secure than the previous IBE system.
Boneh and Franklin[2] proposed a system that was based on BDH and Random Oracle where the adversary made semantic selection of the identity to attack. The drawback of this system was that, the identities were seen as bit strings. As a result, bilinear maps were required for every bit in the identity. Boneh and Franklin used Gentry IBE [5] to base their work on. Canetti et al [6] in 2004, had previously proposed a slightly weaker model where the adversary had to commit in advance to the identity that they wanted to attack. This was also used by Boneh and Boyen to base their system on. In the year 2006, Boneh and Canetti et al. [7] proposed an improved system to the previous [6]. In the proposed systems by Boneh and Boyen[3], no bilinear computation is required. Decryption of the encrypted message requires atmost only 2 computations.
First is based on the Decision Bilinear Diffie-Hellman Assumption (DBDH). This is provides the Selective Identity Secure Hierarchical IBE without Random Oracles.Second is based on Decision Bilinear Diffie-Hellman Inversion (DBDHI) Assumption. This system has the similar cipher text size and encryption time to that of the previous IBE system. It is however, much more efficient. Makes the system hierarchical which again increases security in terms of depth. However this is also a drawback, as the depth in hierarchy increases exponentially and complicates the system. Further, the system was deemed highly impractical in terms of its implementation and usage.

D. Fuzzy identity based encryption:

In 2004, Amit Sahai and Brent Waters [8] proposed an IBE system based on Fuzzy logic. Here, the identity was seen as a set of descriptive attributes. It allows a private key encrypted with a particular identity to decrypt the message of another private key, only if the two identities are close, on measuring with a “set Overlap” distance metric. This scheme is widely used in Biometric systems as Fuzzy IBE has a high tolerance for error and biometric images, usually have a lot of noise included in them. This system is also secure against collision attacks. However, it is not very suitable for WSN since, a lot of storage is required for the information. This is one of the main drawbacks for this system.

E. Identity based online offline encryption (ibooe)

In 2008, FuchunGuo, Yi Mu and ZidenChen [9] proposed a new way of implementing IBE system: Online/Offline IBE systems.In this system, the signing process was divided into two parts, online and offline.The first part of encryption is performed Offline. This phase does not require the actual message for encryption. Most of the

DOI 10.17148/IJARCCE.2017.6163

computational processes are performed in the offline phase. The online phase is performed after the message is known. This phase is faster than the offline phase. IBOOE is based on Boneh-Boyen [3] IBE and the Gentry IBE [5] which itself was an improvement on the Waters IBE system [8]. The system makes use of Decision Bilinear Diffie-Hellman Assumption (DBDH). The system is Chosen Ciphertext Attack (CCA) secure.
Since most of the computation is done in the offline phase, and the message is not required, the computation overhead and storage requirements is very low. There is less chance of the key being intercepted, as, the key is generated usingthe users identity and a set of random selected parameters by the PKG. This leads to high performance. As the storage requirements are very low, this system is highly suited to WSN systems.

In the same year, 2008, Liu,Xu, Zhengren Liu, Zhidechen, Yi Mu and FuchunGuo [10]suggested a Hierarchical ID based Online/Offline Encryption scheme which was based on Boneh-Boyen and Gho [4]. Here, the system was built in a hierarchical manner, where, the public key was seen as “a multi tuple vector of domain identities” This scheme also used Selective Identity which was secure under Decision Bilinear Diffie-Hellman Inversion (DBDHI) Assumption. With this scheme, the ciphertext size was fairly reduced, making it highly suitable for devices with low storage capacity and devices with low computation capability. However, this scheme requires the user to choose the ID it wants to attack beforehand.

In 2008, JoonsangBaek, Han Chiang Tan, Jianying Zhou and Jun Wen Wong [11] proposed the first ever system to realize statefulPublic Key Encryption (PKE) in WSN. Under this scheme, they used indexing as a method to reduce the communication overhead. The repeated part of the cipher text was usually replaced by a short string.It used Elliptic Curve Cryptography ECC, due to the small size of cipher text (160 bytes) instead of the usually preferred RSA algorithm (1024 bytes) for ciphertext generation. One of the main advantages of this system was that, it provided a way to implement Public Key Cryptography (PKC) in WSN which brought simplicity and efficiency. This system provided high level of confidentiality to WSN. Also, due to the use of PKC, the process of decrypting the data was not performed by the sensor nodes, thus, removing the need to store the long-term private key by them.

Chu, Liu, Zhou, Bao and Deng [12] in 2010 proposed a similar system for IBOOE to be used specifically for WSN with stateful PKE. This method increased the encryption speed by allowing the sensors to maintain a “state”. This state was re-used throughout the encryption process for the sensors. This system was based on Diffie-Hellman Assumption and reduced the computation cost for the sender greatly. IBOOE has also been used to mitigate Phishing in email as shown by Ren, Mu and Susilo in 2008 [13].

Phishing is a cybercrime, where fraudulent emails, seemingly from reputable companies are sent to individuals, in order to fool them into revealing confidential information about them, like their bank account credentials, credit card numbers, passwords etc. The proposed system suggests using Identity based Authentication for the sender of the email. Again, the computational overhead is largely reduced since it is performed offline. It also reduces key exposure, which was a drawback of the previous systems.

IV. COMPARATIVE ANALYSIS

In this section, we present a comparative study of the various schemes discussed previously, in table 1.

TABLE 1 COMPARATIVE ANALYSIS OF VARIOUS IBE SCHEMES

S.No	AUTHOR	TECHNIQUE	FEATURES	ADVANTAGES	DRAWBACKS
1.	A.Shamir (1984) [1]	Identity based cryptosystem and signature scheme	• IBS based on integer factorizationproblem and RSA • Unable to implement IBE	• Eliminated the need for a third party intervention • Reduced the cost of PKG maintenance	• Required the user to be aware of the smart card used for encryption. • Was unable to implement IBE
2.	D.Boneh, M.Franklin (2001) [2]	Identity based encryption from weil pairing	• computationally efficient based on Bilinear non degenerate maps • Easy to calculate results • Bilinear diffie-hellman assumption	• No preparation to be made by the receiver • PKI maintenance not required • Makes use of signatures. • Higher security available for PKG	• Key escrow • Needs PKG availability all the time

DOI 10.17148/IJARCCE.2017.6163

3.	Dan Boneh and Xavier Boyen (2004) [3]	Selective ID secure encryption without random oracle.	• 2 models proposed. Both selective ID secure. • First is an extension of HIBE and second is more efficient, based on DBDHI.	• Follows similar encryption and cipher text as IBE • Only 1 pairing computation for decryption • Eliminates the use of random oracles • Reduced cipher text size.	• Highly impractical • Theoretical construct to prove the possibility of of a fully secure IBE without random oracle.
4.	Boneh, Boyen and Gho (2005) [4]	Hierarchical identity based encryption.	• Selective identity secure under DBDHI Assumption. • Does not use random oracle.	• Supports limited delegation of private keys • Low size of cipher text • CCA secure	• Degraded proof of full security • Depth increases exponentially
5.	Amit Sahai, Brent Waters (2004) [8]	Fuzzy identity based encryption	• Based on fuzzy logic • ID's are used as a set of descriptive attributes	• Private key of one identity can decrypt messages of another identity, given their distance as compared by "set comparison" is close • Useful for biometrics • High error tolerance • Secure against collision attacks	• Can only be used for biometric systems. • Not very suitable for WSN as it requires a large database.
6.	FuchunGuo, Yi Mu, Zhide Chen (2008) [9]	Identity based online/offline encryption	• signing process has been divided into 2 • Offline phase does not require the message • Based on Boneh and Boyen and Gentry IBE	• Useful for low powered devices like smart cards hence highly suitable for WSN • Does not require receiver ID for computation • Online computation very fast • CCA secure	Can become impractical and highly user dependent.
7.	Chen-Kang Chu, Joseph K Liu, Jianying Zhou, Feng Bao, Robert H.Deng (2008) [12]	Practical ID based encryption for WSN	• Based on state-full PKE • Based on Diffie-Hellman assumption • Receiver bounded OOIDBE proposed	• Useful for low powered devices • low computation cost for sender • low pre-computational storage • Reduced amount of cipher text • Reuse of previous information	Low flexibility in terms of usage.

V. CONCLUSION

We have seen, the various Identity Based Encryptions that are being implemented and have been used. IBE Systems are highly secure, flexible, Robust and are very suitable for Wireless Sensor Networks. IBE systems make use of the users own identity for the public key instead of random generated attributes. This makes the system very easy to use, even by those who are not aware of the working of the algorithm. As we now know, IBE allows anyone to create a general public key, using their identity. IBE makes use of a third party (PKG) to generate the private key. The PKG keeps hold of the master private key and generates a private key for the requesting user, if he has the valid public key. Hence, encryption can be performed by anyone, as, encryption does not require the public key of

DOI 10.17148/IJARCCE.2017.6163

all the participants. There have been several systems proposed and various improvements made. All in all, the system is very Secure, provides high performance, and low storage capabilities. Because IBE allows encryption to occur, without requiring the public key, this feature led to the creation of online/offline algorithms. However, it is not possible to break down every IBE system into online and offline phases, as, IBE requires prior knowledge of the message to be encrypted and the private key, before encryption can becompleted. Online/Offline systems are the new emerging trend in IBE systems. This field is fairly new and has a high potential for research in the future.

ACKNOWLEDGEMENT

I am grateful to my professors **Ms. Charu Wahi** and **Ms. Seema Sharma** for providing me the opportunity to study and write this paper, and for guiding me throughout.

REFERENCES

[1] Shamir, A., “Identity-based cryptosystems and signature schemes”, Proceedings of Advances in Cryptology - CRYPTO 1984, volume 196 of LNCS, pages 47–53. Springer-Verlag, 1984.

[2] Boneh, D. and Franklin, M., “Identity-Based Encryption from the Weil Pairing”, Proceedings CRYPTO 2001, volume 2139 of LNCS, pages 213–229. Springer-Verlag, 2001

[3] Boneh, D. and Boyen, X., “Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles”, Proceedings of Advances in Cryptology EUROCRYPT 2004, volume 3027 of LNCS, pages 223–238. Springer-Verlag, 2004

[4] Boneh D., Boyen X. and Goh E., Advances in Cryptology EUROCRYPT 2005, volume 3493 of LNCS, pages 440-456, Springer, 2005.

[5] Gentry, C., “Practical identity based encryption without random oracles”, Eurocrypt-2006 volume 4004 of LNCS, pages 445-464, Springer-Verlag 2006.

[6] Canetti R., Halevi S., Katz J., “Chosen cipher-text security from identity based encryption”, Proceedings of Eurocrypt 2004.

[7] Boneh D., Canetti R., Halevi S., Katz J., “Chosen cipher-text security from identity based encryption”, June 13.2006.

[8] Sahai, A., Waters, B., “Fuzzy Identity Based Encryption.” Proceedings of Eurocrypt-2005, Vol. 3494 of LNCS, pages 457-473, Springer-Verlag 2005.

[9] Guo F., Mu Y., and Chen Z., “Identity-based online/offline encryption”, Proceedings of Financial Cryptography and Data Security (FC ’08), volume 5143 of LNCS, pages 247–261. Springer, 2008

[10] Liu Z., Xu L., Chen Z., Guo F., “Hierarchical identity-based online/offline encryption”, International Conference for Young Computer Scientists, University of Wollongong, 2008.

[11] Baek J., Tan H. C., Zhou J., and Wong J. W., “Realizing Stateful Public Key Encryption in Wireless Sensor Network”, Proceedings of The IFIP TC-11 23rd International Information Security Conference (SEC ’08), pages 95–107. Springer, 2008.

[12] Chu C. K., Liu J. K, Zhou J., Bao F., and Deng R. H., “Practical ID-based Encryption for Wireless Sensor Network”, Proceedings of the 5th ASIACCS 2010, page 337-340, 2010.

[13] Ren Q., Mu Y., Susilo W., “Mitigating phishing with ID based online offline authentication”, Published in L.BrankovicM.Miller (EDs.), Australasian Information Security Conference, page 59-64, Wollongong, Australian Computer Society Inc.

[14] Wikipedia website [Online]: Available: https://en.wikipedia.org/wiki

DOI 10.17148/IJARCCE.2017.6163