Advantages of an Efficient Certificate Less Signature Scheme Over Identity-Based Signature Scheme

Ashish Savita
CSE Department
Rama University, Kanpur
kitashishcse@gmail.com

Sandeep Singh
CSE Department
Rama University, Kanpur
er.sandeepkanpur@gmail.com

C.Rama Krishna
CSE Department
NITTTR, Chandigarh
rkc_97@yahoo.com

***Abstract*- Nature and resource limitations of sensor nodes deployed against anti suffer from physical attacks to secure these nodes raise some serious questions. Random failure of nodes in real life deployment scenarios. Due to lack of resources in sensor nodes, computation and communication overhead with large traditional security mechanisms are infeasible in WSNs. In the case of a compromise KGC prevent a complete breakdown of the system, the key generation process is divided between KGC and users. Moreover efficient key distribution and management system is lightweight ciphers also needed. Several key establishment technique limited memory and is designed to address the tradeoff between securities, but the plan has been the most effective is still debatable. In this paper, we analyze the various authentication protocols. .**

Keywords- Wireless Sensor Network, security; Authentication Protocols Online/Offline.

.

I. INTRODUCTION

A signature scheme is always used with transmitted information to ensure that sensitive information has not been modified by an adversary. Traditional signature schemes allow a signer to sign a message using his/her private key. Shamir [1] in 1984 first developed an identity-based cryptosystem Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value.

To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to Generate the private key for identity ID.As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints.

However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt (or sign) messages without authorization.

Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow.

(Key Distribution)[5].

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

- Node authentication: Ideally, the key management technique should guarantee that the communicating nodes are able to verify each other's identity in a secure way. This feature helps the network to pinpoint misbehaving nodes, resulting in a higher resistance against the capture of valid nodes and attempts of impersonating them.
- Resilience: Refers to the resistance of the scheme against node capture, where an adversary physically attacks a sensor and recovers secret information from its memory. The scheme's resilience is given by the fraction of the network communications that are exposed to the adversary,[9] excluding the communications in which the compromised node is directly involved.
- Node revocation: Upon the discovery of compromised nodes, the key management solution should provide efficient ways to dynamically revoke them from the network. Such mechanisms are useful to prevent an adversary from inserting malicious nodes into the network, even if this adversary

obtained access to some secret information (e.g., through node capture).

• Scalability: During the sensor network lifetime, its size may vary dynamically; thus, the key distribution scheme must support large networks and, at the same time, allow the introduction of new nodes without loss of security.

II. KEY MANAGEMENT

Key management is a crucial part of security in WSN and has been densely researched recently. Key management is a fundamental security issue in sensor networks. It is the basis to establish the secure communication using cryptographic technologies between sensor nodes in a sensed area. Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed. [4]There are many principal concerns in a key management framework:

• Key deployment: How many keys are needed to be deployed in the network?

• Key pre-distribution phase: This phase is carried out before the deployment of the network, more precisely during the node's manufacturing time.

• Key establishment: How does any pair of nodes or a group of nodes establish a secure session?

• Network initialization phase: Comprise the very first steps required in order to setup the network's security, and it is performed during the network Deployment.

• Member/node addition: How should a node be added to the network such that it be able to establish secure sessions with existing nodes in the network, while not being able to decipher past traffic in the network?

• Member/node eviction: How should a node be evicted from the network such that it will not again be able to establish secure sessions with any of the existing nodes in the network, and not be able to decipher future traffic in the network?

• Authentication protocol: it is carried out every time a new node requests to join the network, once the previous phase has finalized.

III. DIFFICULTIES IN CERTIFICATELESS SIGNATURE SCHEME

In a Certificateless signature scheme, the security is assessed in terms of two different kinds of attackers. The first kind of attacker (or Type I attacker) is meant to represent a normal third party attack against the existential unforgetability of the system.

Due to the uncertified nature of the public-keys produced by the users, one must assume that the attacker is able to replace these entities public keys at will. This represents the attackers' ability to fool a user into accepting a signature using a public key that has been supplied by the attacker.

Therefore, a Certificateless signature is required to be secure against key Replacement attack, a third party who can replace the user's public/secret key pair but does not know the user's partial private key issued by the KGC cannot generate valid signatures as the user either.

The second kind of attacker (Type II attacker) represents a malicious key generation center, which is given the key generation center's long term secret, but may not replace entities' public keys.

IV. SCHEMES WHICH IMPROVE CERTIFICATE LESS SIGNATURE SCHEME

Scheme can be classified in one of three general groups, Self-enforcing Schemes, Arbitrated Keying Schemes & Pre-distribution Schemes.

• Self-enforcing Schemes use asymmetric cryptography in order to establish keys after deployment. The main drawback of this strategy refers to the performance of most asymmetric algorithms currently available: although a considerable effort devoted to the adaptation of public key cryptography to highly constrained devices, both through the use of certificates and elliptic-curve cryptography (ECC) [2][4], it is still unclear if the amount of resources necessary even for highly optimized implementations is already low enough for a wider acceptance of this approach.

• Arbitrated Keying Schemes rely on a trusted central point (e.g., a base station) for key establishment and management. An issue with this strategy is that the central point becomes a preferred target for attacks that, if successful, can disrupt the entire network. Nonetheless, when such a trusted point is available (which is often the case in heterogeneous hierarchical WSNs) and can be considered secure, these schemes become very attractive.

• Pre-distribution Schemes, an especial entity known as Key Distribution Center (KDC) is responsible for loading the keys into the sensor nodes prior to deployment, which can be done either through their physical or wireless interfaces. The reasoning behind this strategy is to avoid the overhead that could be originated from dynamic key generation processes. Moreover, this approach results in a network with little or no dependence on a central station after the nodes are deployed. For these reasons, this strategy is usually considered more adequate for WSNs.

choe et al. Developed an efficient short CLS scheme. the CLS scheme by He et al. cannot withstand a strong type 2 adversary. . Li et al. , Zhang et al. [3] and Gorantla and Saxena [4] proposed a new CLS scheme using bilinear pairings.

V. EVALUATIONS OF KEYING PROTOCOLS

In this section, we define the most common metrics used for the evaluation of key management networks, we evaluate how the network scales up to the imposed limit (hence, we can have a high value techniques in WSNs. While some of these metrics are very general, others are originated from the requirements imposed by the several constraints inherent to these systems. These metrics can be classified in three main groups, which define the (usually conflicting) requirements to which they are associated: security, scalability and efficiency.

Key management schemes must provide the secret keys in a secure way, thwarting the activities of malicious nodes in the network. In this sense, they must assure that only secure entities are able to assign and/or update keys in the network, preventing external sources from doing so. Moreover, the solution must prevent the disclosure of the keys to unauthorized parties.

TABLE I COMPARATIVE ANALYSIS OF AUTHENTICATION PROTOCOLS WITH NODE

Authenti cation Protocol	**Node authenticat Ion(Na)**	**Resilien ce(R)**	**Node Revocati On(Nr)**	**Scalabil ity(S)**
SPINS	YES	100%	Easy	Worst
LEAP	YES	100%	Easy	Worst
CAGKA	YES	0%	Very difficult	Excelle nt

VI. RELATED WORK

Comparison Table displays a list of the Protocols considered in this survey, as well as summarizes our security analysis, considering the following aspects.

{Na}: if node to- node authentication is supported; schemes marked as ‘‘yes” are those that support such feature only after the initial key establishment. {R}: percentage or number of nodes compromised when a single node is captured before it is able to remove any redundant information (e.g. an already used key) from its memory.

{Nr}: how difficult it would be to revoke a node. {S}: rank evaluating the maximum amount of nodes supported by the network; higher values mean better scalability for a given amount of keys stored and key connectivity achieved; for limited for this parameter even if such a limit exists).

Al-Riyami and Paterson [2] developed a Certificateless cryptosystem to overcome weaknesses of identity-based cryptosystems the private key in Certificateless cryptosystem is cooperatively generated by a KGC and a signer. Thus, a strong Certificateless cryptosystem must withstand a malicious KGC, and withstand malicious outsiders who can replace the signer’s public key. Several Certificateless cryptosystems have since been developed.

The KGC first generates a key pair, where the private key is now the partial private key of the system. The remainder of the key is a random value generated by the user, and is never revealed to anyone, not even the KGC.

All cryptographic operations by the user are performed by using a complete private key which involves both the KGC's partial key, and the user's random secret value.

VII. CONCLUSION

Certificateless public key cryptography is receiving significant attention because it is a new paradigm that simplifies the traditional PKC and solves the inherent key escrow problem suffered by ID-based cryptography. Certificateless signature is one of the most important security primitives in CLPKC.

REFERENCES

[1] A. Shamir, Identity-based cryptosystems and signature schemes Proceedings of CRYPTO 84 on Advances in Cryptology, Santa Barbara, California, USA, 1984; 47–53.

[2] S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography Proceedings of ASIA CRYPT 2003, Taipei, Taiwan, 2003; 452–473.

[3] Z. Zhang, D.S. Wong, J. Xu and D. Feng, “Certificateless public-key signature: Security model and efficient construction”, Proc. of CAN 2006, Lecture Notes in Computer. Sci., vol. 3989, pp. 293–308, 2006.

[4] M.C. Gorantla and A. Saxena. An efficient Certificateless signature scheme 2005 International Conference on Computational Intelligence and Security, Xi’an, China, 2005; 110–116.

[5] S. S. Al-Riyami and K. G. Paterson (2003), "Certificateless Public Key Cryptography", Proc. of Asiacrypt 2003, LNCS, Vol. 2894,.