Survey on Efficient and Forward Secure Schemes for Unattended WSNs

Shibin D, Blessed Prince P

Abstract: - Unattended Wireless Sensor Networks face challenges in providing good security and in showing good performance. The lack of communication with the final data receivers is the main reason for this. It is possible for the UWSNs to gather the sensible data for long time. These data are vulnerable to adversaries who can compromise the sensors and maneuver the sensed data. This paper describes how various methodologies are used to act against the adversaries troubling the UWSNs. The various cryptographic measures have to take the vulnerabilities into consideration thus making the network improve its performance and security. In this survey paper, a detailed study about the various schemes that increase the efficiency and performance of UWSNs and the measures taken to improve forward security are given.

Keywords- Aggregate Signature, Digital Signatures, Forward-Secure Property, HaSAFSS Scheme, Keying materials, Overhead, Unattended Wireless Sensor Networks.

I. INTRODUCTION

A WSN consists of densely distributed nodes that support sensing, signal processing [1], embedded computing, and connectivity; sensors are logically linked by self organizing means [2-6]. In wireless sensor network provides the following services such as monitoring, alerting, information on-demand and actuating [7]. On the other hand, unattended wireless Sensor Networks faces lack of communication because of its nature.

An Unattended Wireless Sensor Network is one in which continuous end-to-end real time communication is not possible for the senders and the receivers [8]. Sometimes the receivers may not be available for the sensors and hence the sensors gather the sensible data and send it when the receivers are available. The best example for the UWSNs could be seen in military applications where they deploy the sensors in an unattended environment to gather the sensed data.

In UWSNs, Security can be achieved by cryptographic measures like Key management, secure routing and prevention of Denial of Service (DOs) [7]. But when a node is compromised, the keys for communicating with other nodes also compromised, hence the node cannot be identified whether it is genuine or not by simply employing cryptographic measures [7].

There are challenges in improving computational efficiency, public verifiability, forward security, scalability. The survey has been done based on providing security and to achieve the above mentioned goals.

II. TERMINOLOGIES

A. Forward-Secure property

The **forward-security property** means that even if the adversary obtains the current secret key, she still cannot forge signatures for past time periods.

B. Unattended Wireless Sensor Networks

Unattended Wireless Sensors are those which face lack of communication because of the unavailability of the receivers. Hence it accumulates the sensed data and transmits it whenever the receiver is available.

C. Overhead

Overhead is the combination of the excessive computation time, memory and bandwidth that are required to attain a particular goal [9].

D. Keying Materials

The data necessary to establish and maintain cryptographic keying relationships. Examples such as Initialization vector, keys, etc.

E. Aggregate Signature

A Signature Scheme that supports aggregation. Given n signatures on n messages from n users, it is possible to aggregate all these signatures in to a single signature whose size is constant in the number of users and this single signature will convince the verifier that the n users did indeed sign the n original messages [10].

F. HaSAFSS Scheme

HaSAFSS schemes utilize existing verification delays in UWSNs to introduce asymmetry between signers and verifiers. In this way, they integrate the efficiency of mac-based aggregate signatures and the public verifiability of bilinear map based signatures by preserving the forward security via timed-release encryption (TRE).

G. Digital Signature

A digital signature is a scheme for demonstrating the authenticity of a digital message and a valid digital signature gives recipient reason to believe that the message was created by known sender such that they cannot deny sending it and the message was not altered in transit [10].

Manuscript published on 28 February 2013.
***Correspondence Author(s)**

Mr. Shibin D, Post Graduate Scholar, Department of Information Technology, Karunya University, Coimbatore, India.
Mr. P. Blessed Prince, Assistant Professor (SG), Department of Information Technology, Karunya University, Coimbatore, India.

H. Trusted Third party

Trusted Third party (TTP) is an entity which encourages the interaction between two parties who trust the third party.

I. Public Key Infrastructure

Public Key Infrastructure is an array that gathers public keys with respective user identities by means of a certificate authority.

II. CLASSICAL METHODOLOGIES FOR FORWARD-SECURE AND EFFICIENT UWSNs

There are various methodologies under the wireless sensor networks for providing forward security and to improve the efficiency. Few such methodologies are discussed here.

A. Forward-Secure Sequential Aggregate MAC Scheme

To ensure forward security and to minimize resource consumption, the Forward-Secure Sequential Aggregate authentication Schemes have been introduced in [11]. It can be used to authenticate multiple messages when public (transferrable) verification is not required.

If public (transferrable) verification is required we need an FssAgg signature scheme to check the authenticity of data records. The advantages can be MAC based scheme is highly efficient and both key exposure will be there along with good storage efficiency.

B. Co-GDH Scheme

A Co-GDH signature is a single element of any group which is half the size of the DSA signatures with similar security [12].

On certain elliptic curves these signatures are very short. It comprises of three algorithms such as KeyGen, Signing and Verification. These three schemes comprised together forms a Co- Gap Diffie Hellmen scheme. It doesn’t need any verification methodologies.

C. Trusted Agent

The goal is to encrypt a message so that it cannot be decrypted by any person not even the sender in anticipation of a pre determined amount of time has passed. Here comes the action of a trusted agent and its functioning.
A Trusted Agent is a member of your organization who manages ECA Certificate enrollments [8]. The Trusted Agent ensures that your enrollment information is valid and accurate, which enables faster issuance of your ECA Certificate. Often the Trusted Agent also assumes the role of the notary by notarizing the Subscriber Enrollment Form. We can efficiently enable timed release crypto.

D. TESLA

TESLA is an efficient broadcast authentication protocol that also uses delayed disclosure of the keying material, assuming that signers and verifiers are loosely synchronized. However, our schemes provide important properties that are not obtainable in TESLA [8].
First, in TESLA, an attacker ‘A’ that compromises a signer can easily forge all previously accumulated data items in a given time interval, since asymmetry is directly introduced by the signer. However, HaSAFSS schemes protect previously accumulated data items via mechanisms that achieve forward security. Moreover, TESLA generates an individual signature for each individual data item; however, HaSAFSS schemes compute an aggregate signature for multiple data items, which reduces the storage and communication overhead. Finally, HaSAFSS schemes also achieves the ‘‘all-or-nothing’’ property due to the signature aggregation, which is not available in TESLA.

E. Timed Release Encryption (TRE)

The purpose of TRE is to encrypt a message in such a way that no entity, including the intended receivers, can decrypt it until a pre-defined future time [8]. The majority of modern TRE schemes are based on Trusted Agent (TA), in which a time server provides universally accepted time reference and trapdoor information to users.
Hence, users can decrypt the cipher text when its related trapdoor information is released by the TA. Most of the recent TRE schemes are based on Identity- Based (IB) cryptography.

F. Secure Logging

It investigates the concept of immutability in the context of forward secure sequential aggregate authentication to provide finer grained verification [7].
The need for secure logging is well-understood by the security professionals, including both researchers and practitioners. The ability to efficiently verify all (or some) log entries is important to any application employing secure logging techniques.

G. BAF and FI-BAF schemes

Blind-Aggregate-Forward (BAF) and Fast-Immutable BAF (FI-BAF) logging schemes, which are suitable for large distributed systems. BAF can produce publicly verifiable forward secure and aggregate signatures with near-zero computation, signature storage, and signature communication overheads for the loggers, without requiring any online Trusted Third Party (TTP) support [6]. FI-BAF extends BAF by allowing selective verification of log entries without compromising the security of BAF as well as retaining its computational efficiency.

H. Self Healing Technique

Self Healing means the ability to detect failures and compensate for them if possible, and adapt to a changing environment as well as to changing objectives. The detection of node failures is a generic, non-trivial task in distributed environments [8]. In this work a new failure detection algorithm has been proposed. A failure recovery engine has been developed to manage distributed systems and recover them from unwanted states.

I. HASAFSS – Security Scheme

The goal of HaSAFSS schemes is to achieve secure signature aggregation and forward security simultaneously. The previous schemes focuses on forward-security, existential unforgeability and authentication properties, to analyze our schemes [8]. The forward-security objective of HaSAFSS schemes is slightly different than that of previous forward-secure and aggregate schemes. That is, HaSAFSS aims to achieve a time-valid forward-security instead of a permanent forward-security.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

IV. COMPARISION OF VARIOUS REFERENCE PAPERS

SNo	TITLE	OBJECTIVE	TECHNIQUE	MERITS	DEMERITS
1.	Self-Sustaining, efficient and forward secure cryptographic constructions for unattended wireless sensor networks	To find a new class of cryptographic schemes, referred to as Hash-Based Sequential Aggregate and forward secure signature (HaSAFSS) which allows a signer to sequentially generate a compact, fixed size and publicly verifiable signature efficiently.	1.Symmetric HaSAFSS, 2. ECC based HaSAFSS and 3. self sustaining HaSAFSS	1. High computational efficiency 2. public verifiability, 3. signature aggregation 4. forward secure integrity	1. Low storage 2. communication overhead
2.	Forward-Secure Sequential Aggregate Authentication	To ensure forward security and to minimize resource consumption, the Forward-Secure Sequential Aggregate authentication Schemes have been introduced.	1.Forward-Secure Sequential Aggregate MAC Scheme	1.MAC-based scheme is efficient	1.Signature based scheme is not efficient 2.lower verification complexity
3.	A Forward-Secure Digital Signature Scheme	The ideas from the Fiat-Shamir and Ong-Schnorr identi_cation and signature schemes, and is proven to be forward secure based on the hardness of factoring, in the random oracle model is constructed.	Forward Secure Sequential Aggregate MAC scheme	Highly Efficient	Digital Signature is efficient but with lower verification complexity
4.	A New Approach to Secure Logging	It investigate the concept of immutability in the context of forward secure sequential aggregate authentication to provide finer grained verification	1. Time lock puzzles	1. Public verifiability, 2. signature aggregation	lower verification complexity
5.	Aggregate and Verifi ably Encrypted Signatures from Bilinear Maps	To show that aggregate Signatures give rise to verifiably encrypted signatures. Such signatures enable the verifier to test that a given ciphertext C is the encryption of a signature on a given message M. Verifiably encrypted signatures are used in contract-signing protocols.	1.Co-GDH Signature Scheme 2. Bilinear Maps	Key generation, aggregation, and verification require no interaction.	Chances are there to forger the message
6.	Time lock puzzles and timed release Crypto	Our motivation is the notion of timedrelease crypto where the goal is to encrypt a message so that it cannot be decrypted by anyone not even the sender until a redetermined amount of time has passed	1.Timelock puzzles 2. Using trusted agents	We can efficiently enable timed release crypto	Time constraints are there

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

7.	Hash-Based Sequential Aggregate and Forward Secure Signature for Unattended Wireless Sensor Networks	To show that the schemes such as HASAFSS are significantly more efficient in terms of both computational and storage overheads than previous schemes for highly resource constrained UWSN applications.	1.Time Trapdoor Release 2. Sym-HaSAFSS and ECC-HaSAFSS	1. Efficient in cost, storage	2. Computational overheads occur
8.	Identity-Based Encryption from the Weil Pairing	The scheme has chosen ciphertext security in the random oracle model assuming an elliptic curve variant of the problem	1.Weil Diffie-Hellman Assumption 2. Identity based encryption	1. ciphertext security for identity-based systems	DDH assumption is false

V. CONCLUSION

In this paper, we have discussed the various methodologies that ensure forward-security and give more efficiency. Also the applications of these schemes deal with the key management in unattended wireless sensor networks. Even though forward-security prevents key compromises, the various hashing schemes which were discussed in the latter part of the paper gives a satisfaction that it is the best. Hence the survey has covered all the corners of the UWSNs to make it efficient and forward-secure.

REFERENCES

1. R. Nowak, U. Mitra, ‘‘Boundary Estimation in Sensor Networks: Theory and Methods,’’ Proceedings of the 2nd Workshop on Information Processing in Sensor Networks (IPSN’03), Palo Alto, CA, Apr. 2003.
2. K. Sohraby et al., ‘‘Protocols for Self-Organization of a Wireless Sensor Network,’’ IEEE Personal Communications, Vol. 7, No. 5, Oct. 2000, pp. 16ff.
3. A. Cerpa, D. Estrin, ‘‘ASCENT: Adaptive Self-Configuring Sensor Networks Topologies,’’ Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (InfoCom’02), New York, Vol. 3, June 2002.
4. H. Gupta et al., ‘‘Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution,’’ Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc’03), Annapolis, MD, June 2003.
5. Q. Huang et al., ‘‘Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks,’’ Proceedings of the 2nd Workshop on Sensor Networks and Applications (WSNA’03), San Diego, CA, Sept. 2003.
6. Kazem Sohraby, Daniel Minoli, Taieb Znati, Wireless Sensor Networks - Technology, Protocol and Applications, Second edition, 1991.
7. G. Edwin Prem Kumar et al, "A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Network" International Conference on Modelling Optimization and Computing, 2012.
8. Attila Altay Yavuz, Peng Ning, “Self-Sustaining, Efficient and Forward-Secure Cryptographic Schemes for Unattended wireless sensor networks,” Ad hoc Networks, Vol. 10, Apr 2012, pp. 1204-1220.
9. http://en.wikipedia.org/wiki/Overhead_(computing)
10. http://en.wikipedia.org/wiki/Digital_signature
11. D. Ma, Practical forward secure sequential aggregate signatures, in: Proceedings of the 3rd ACM symposium on Information, Computer and Communications Security (ASIACCS ’08), ACM, NY, USA, 2008, pp. 341–352.
12. D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, in: Proc. of the 22th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT ’03), Springer-Verlag, 2003, pp. 416–432.