A Survey on security and privacy in Wireless Sensor Network

[1]Sameer Kumar Meher, [2]Leena Das, [3]Manjusha Pandey
[1] Postgraduate Scholar, [2] Assistant Professor, [3] Assistant Professor
[1] School of Computer Engineering,
[1] KIIT University, Bhubaneswar, Odisha, India

***Abstract* - Over the past few years, the concern of security is increasing day by day. Without proper protection, any part of any network can be susceptible to attacks or unauthorized activity. Ring Signature is a type of digital signature that enable a user to sign a message so that ring of possible signers is identified without revealing exactly which member of that ring actually generated the signature.Ring signatures are completely ad-hoc in nature there is no requirement of any central authority or coordination among different users. In this paper, we review summarize the study of ring signature schemes and scrutinize their relationships with other existing cryptographic schemes and discuss the uses and the mechanism used by ring signature.**

***Keywords* - wireless sensor network; ring signature; privacy**

I. INTRODUCTION

In today's world, wireless sensor network plays a vital role in the field of wireless networking. As far as security point of view we need to provide better security to these networks. For securing the wireless sensor network it needs to make the network support all security properties like availability, authenticity, confidentiality and integrity. So various techniques has been proposed to keep the privacy on for sensor networks, one of them was introduced by Rivest, Shamir, and Tauman named as Ring Signature at ASIACRYPT in 2001.

If we talk about the history of this signature, this signature was generated as a proof of solidarity when farmers in a certain village resisted their ruler. The purpose is to hide their leader by making this kind of shape of signature.

The reason why they make this kind of shape as :If members simply signed, the first signer would be suspected of the leader (Since the leader was especially punished, the members were reluctant to sign first).So, members sequentially signed like a Ring, try to hide the order of signers.

In this way, with the help of signature they hide the leader and the members who participate in the signature take equal responsibility. Ring Signature is a type of digital signature that enable a user to sign a message so that ring of possible signers (user itself is a member) is identified without revealing exactly which member of that ring actually generated the signature. Ring signatures are completely ad-hoc in nature there is no requirement of any central authority or coordination among different users.

Moreover, Ring Signatures are similar to group signatures but in two ways :

1. There is no way to revoke anonymity of individual signature.
2. Any group of users can be used as a group without additional setup.

The rest of the paper is arranged as follows:
In Section 2, we visualize the properties of ring signature scheme and the security properties. In Section 3, we discuss the cryptographic schemes its uses and the mechanism used by ring signature. In Section 4, finally we give a conclusion.

II. RING SIGNATURE SCHEME AND THE SECURITY PROPERTIES

There are various kinds of ring signature schemes applied for different purposes, few of them are: An Efficient Strong Designated Verifier Ring Signature Scheme which provides One out of all Signer Anonymity to hide the identity of actual signer. This scheme also provides signer admission to admit that who is the actual signer. [2] Code based Ring Signature Scheme with signature length of 144+126 l bits (l implies the number of ring members), it is one among all the most short ring signature presented ring signature schemes till now. [6] From bilinear pairings an improved ring signature scheme (identity based) where the ring signature is considered as a simplified group signature with few appealing features where no need of manager, no group setup procedure and no revocation mechanism used against signer's anonymity.[3] Over elliptic curve cryptosystem an anonymous signcryption in ring signature scheme, it combines all elliptic curve cryptosystem properties and ring signature. While the signers are endue with properties like anonymity through the technique of ring signature, this cryptosystem achieves the advantages like high security, low computation load and requirements of small bandwidth. [5]

An Efficient Signature Scheme from Bilinear Pairings and its Applications where a new short signature scheme from the bilinear pairings that unlike BLS,it uses some general cryptographic hash functions such as SHA-1 or MD5, and they does not require special hash functions.

Moreover, this scheme requires less pairing operations than BLS scheme and so it is much more efficient as compared to BLS scheme. [7] Identity based Ring Signature Scheme with Enhanced Privacy where the identity based cryptographic techniques doesn't require certificates. Using identity based cryptography the construction of ring signatures allow for privacy preserving digital signatures to be created in application when certificates are not available or desirable such as in vehicle area networks or VANET. Here proposal of a new designated verifier identity based ring signature scheme that is secure against full key exposure attacks even for a small group size. [9]

Security Properties

- Ring signature formalization was given by Yu and Guan (2008) and is defined as follows : [10]
  Ring-sign (m, P1, P2, ...,Pr,s, Ss): With the public keys (P1, P2, ..., Pr) corresponding to ring members (r) along with the secret key (Ss) which is the sth member (actual signer) which produces a ring signature (r) for the message (m). The signer uses a probabilistic algorithm for the signature generation.
- **Ring-verify**: (m, r) The verifier accepts a message (m) and a signature (r) including all the public keys of all possible signers if true, otherwise, rejects the message.
- **Ring signature verification**: It is a deterministic algorithm, which has basically three security requirements.
- **Signer ambiguity**: The probability that a verifier will be unable to determine the real signer of a ring with size (r), is greater than 1/r Hence the anonymity in the ring signature is limited and can be computational or unconditional. When the verifier is not the actual signer it just a participator of the ring then it can guess the actual signer with a probability no greater than 1/(r-1).
- **Correctness**: The verifier satisfies the verification equation whenever a signer correctly generates a ring signature with any of the signature scheme.
- **Unforgeability**: Ring signature possesses strongest definition of unforgeability where any non-ring member trying to forge a ring signature on behalf of other ring members (n) for which the non-ring member is not a part of the message and successful is negligible. Therefore, members who are not part of the signature cannot forge any message. The property of the ring signature indicates that, with the size of any ring the signature grows linearly because the signature must incorporate with the list of ring members.

III. DISCUSSION

In this section we review the uses and the mechanism used by ring signature.

In 1991, Chaum, David, and Eugène Van Heyst. "Group signatures." has shown that what the group signatures are contained of and for what purpose he proposed this type of signature. It proposed four schemes which satisfy all properties of group signatures. The group signatures are a "generalization" of the membership authentication schemes in which one person proves that he belongs to a particular group. [4]

In 2003, Tang, Chunming, Zhupjun Liu and Mingsheng Wang."An improved identity-based ring signature scheme from bilinear pairings” proposed a ring signature scheme which overcomes the issues related to ring signature by C Lin and T Wu which was found unreasonable from bilinear pairings and also found less effective as the parameters are not justified correctly and equations they formed are unreasonable. [3]

In 2004, Zhang, Fangguo, ReihanehSafavi-Naini, and Willy Susilo. "An efficient signature scheme from bilinear pairings and its applications" proposed a new short signature scheme from the bilinear pairings. This scheme is constructed from Inverse Computational Diffie-Hellman Problem (Inv-CDHP) which does not require any special hash function which furnish the BLS (Boneh, Lynn, and Shacham) scheme having a special hash function which is generally inefficient and probabilistic in nature.[7]

In 2006, Bender, Adam, Jonathan Katz, and Ruggero Morselli." Ring signatures: Stronger definitions, and constructions without random oracles “stated few problems such as: Previous definitions of security for ring signature schemes are too weak in accordance with recent and realistic attacks scenarios which they cannot be considered into account.[1]

They have proposed an Efficient 2-User Ring Signature schemes: First, scheme is based on standard signature scheme constructed by Waters. Secondly, scheme is based on Camenisch-Lysyanskaya signature scheme. The study concedes of many definitions, theorems, claims & constructions which led the security level of ring signature schemes (of characteristics).

In future work, we may also add the various ring signature schemes in accordance with the definitions and can define all kinds of realistic attacks on each security characteristics.

In 2006, Wu, Yu Fang Chung1 Zhen Yu, and Feipei Lai1&3. TzerShyong Chen. "Anonymous signcryption in ring signature scheme over elliptic curve cryptosystem" proposed an anonymous signcryption scheme which is based on the elliptic curve cryptosystem which combines elliptic curve cryptosystem and ring signature properties. Signers are endue with anonymity through these techniques of which achieves advantages of high security, low computation load and requirement of small bandwidth .Hence, transmission load is reduced and efficiency of performance and transmission is enhanced. [5]

In 2006, Gamage, Chandana, et al. "An identity-based ring signature scheme with enhanced privacy" proposed some security definitions are applied here to enhance the Identity –Based ring signature scheme with respect to the VANET application as a tool to create privacy preservation for standard ring signature scheme is a remedy to a full key exposure attacks for a small group size and ambiguity problem.[9]

In 2007, Zheng, Dong, Xiangxue Li, and Kefei Chen. "Code-based Ring Signature Scheme" proposed a code based ring signature scheme with signature 144 + 126 l Bits (l = number of ring members used) overcomes hard Syndrome-Decoding problem found in the signature scheme with public key cryptosystem shown by Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier(CFS).[6]

In 2012, Hwang, Shin-Jia, and Jyong-Ye Chen. "An Efficient Strong Designated-Verifier Ring Signature Scheme Providing One-out-of-All Signer Anonymity" proposed an efficient strong designated verifier ring signature scheme with maximal signer anonymity which consists of four algorithms: Setup, Ring-Sign, Ring-Ver and Admission which made the scheme effective from computation cost (ring signature generation is heavy while the size of the ring signature is also large) as providing signer admission and anonymity concurrently.[2]

In 2013, Debnath, Ashmita, Pradheep kumar Singaravelu, and Shekhar Verma " Privacy in wireless sensor networks using ring signature" proposed A ring signature which was to authenticate the source node while preserving its spatial privacy also was to authenticate the source node while preserving its spatial privacy and to determine the effectiveness of the proposed scheme, enhancement in the location uncertainty with a ring signature was evaluated.

Tabular view of all above discussions

Name of Authors	Year of publication	Proposed Mechanism	Features
Chaum, David, and Eugène Van Heyst	1991	Proposed four schemes which satisfies all properties of group signatures.	Only members of the group can sign messages; the receiver can verify that it is a valid group signature, but cannot discover which group member made it.
Zhang, Fangguo, ReihanehSafavi-Naini, and Willy Susilo	2004	Proposed a new short signature scheme from the bilinear pairings.	This scheme is constructed from Inverse Computational Diffie-Hellman Problem (Inv-CDHP) which does not require any special hash function.So less computational load to perform tasks.
Bender, Adam, Jonathan Katz, and Ruggero Morselli	2006	Proposed New defniitions of anonymity and unforgeability, Efficient 2-User Ring Signature scheme.	Powerful definitions, theorems, claims and constructions which led the security level of ring signature scheme.
Wu, Yu Fang Chung1 Zhen Yu, and Feipei Lai1&3. TzerShyong Chen	2006	Combines properties of elliptic curve cryptosystem and ring signature.	Advantages of high security, low computation load and requirement of small bandwidth.
ChandanaGamage, Ben Gras, Bruno Crispo, and Andrew S Tanenbaum	2006	Security definitions for standard ring signature scheme are applied with Full key exposure attacks for a small group size and ambiguity problem.	To enhance the Identity -Based ring signature scheme with respect to the VANET application as a tool to create privacy preservation.
Zheng, Dong, Xiangxue Li, and Kefei Chen	2007	Code based ring signature scheme with signature 144 + 126 l Bits (l = number of ring members used).	Signature length and the verification cost will always remain extremely small. The unique features make our coding-based ring signature scheme an exclusive choice for some applications.
Hwang, Shin-Jia, and Jyong-Ye Chen	2012	Proposed efficient strong designated-verifier ring signature scheme providing maximal signer anonymity.	Improves the performance of Hwang and Cheng's scheme.
Debnath, Ashmita, Pradheepkumar Singaravelu, and Shekhar Verma	2013	A ring signature was proposed to authenticate the source node while preserving its spatial privacy.	It have a small overhead and not to adversely affect the performance of the sensor network

IV. Conclusion

This paper addresses the study of Ring Signatures, how they can make use of themselves in wireless sensor network by applying their schemes their relationships with other existing cryptographic schemes and mechanisms used by ring signature to provide better security in future and enhance the level of security for sensor networks.

REFERENCES

[1] Bender, Adam, Jonathan Katz, and Ruggero Morselli. "Ring signatures: Stronger definitions, and constructions without random oracles." Theory of Cryptography.Springer Berlin Heidelberg, 2006.60-79.

[2] Hwang, Shin-Jia, and Jyong-Ye Chen. "An Efficient Strong Designated-Verifier Ring Signature Scheme Providing One-out-of-All Signer Anonymity." Journal of Applied Science and Engineering 15.4 (2012): 381-390.

[3] Tang, Chunming, Zhupjun Liu, and Mingsheng Wang. "An improved identity-based ring signature scheme from bilinear pairings." NM Research Preprints (2003): 231-234.

[4] Chaum, David, and Eugène Van Heyst. "Group signatures." Advances in Cryptology—EUROCRYPT'91. Springer Berlin Heidelberg, 1991.

[5] Wu, Yu Fang Chung1 Zhen Yu, and Feipei Lai1&3. TzerShyong Chen. "Anonymous signcryption in ring signature scheme over elliptic curve cryptosystem." (2006).

[6] Zheng, Dong, Xiangxue Li, and Kefei Chen. "Code-based Ring Signature Scheme." IJ Network Security 5.2 (2007): 154-157.

[7] Zhang, Fangguo, Reihaneh Safavi-Naini, and Willy Susilo. "An efficient signature scheme from bilinear pairings and its applications." Public Key Cryptography–PKC 2004.Springer Berlin Heidelberg, 2004.277-290.

[8] Meiklejohn, Sarah. "An Exploration of Group and Ring Signatures."UCSD Research Exam (2011).

[9] ChandanaGamage, Ben Gras, Bruno Crispo, and Andrew S Tanenbaum."An identity-based ring signature scheme with enhanced privacy."Securecomm and Workshops, 2006. IEEE, 2006.

[10] Debnath, Ashmita, Pradheepkumar Singaravelu, and Shekhar Verma. "Privacy in wireless sensor networks using ring signature." Journal of King Saud University-Computer and Information Sciences (2014).