RESEARCH PAPER | Computer Science | Volume : 5 | Issue : 8 | August 2015 | ISSN - 2249-555X

Source Privacy and Compromise- Resilient Message Authentication in Wireless Sensor Networks

KEYWORDS: Blind Signature, Source Privacy, Data Security

K.Dhanalakshmi
M.Phil in Research Scholar, Department of Computer Science and Engineering,Alagappa University,karaikudi,Tamil Nadu.

Dr.K.Kuppusamy
Professor, Department of Computer Science and Engineering, Alagappa University, Karaikudi,Tamil Nadu.

ABSTRACT *Authentication is any process of system verifies the identity of the user access information. Source privacy is an important to the network security. Network security validate by a provisions and policies. The provisions and policies mainly used to authorize person access the information. Message authentication is a standout amongst the best approaches to defeat unapproved and undermined messages from being sent in wireless sensor systems. Hence, various message verification plans have been produced, based on symmetric-key cryptosystems. The majority of them, not withstanding, have the limits of high computational also correspondence overhead not withstanding absence of adaptability and flexibility to hub trade off assaults.A polynomial-based plan was as introduced. When the quantity of messages transmitted is bigger than this limit, the foe can completely recuperate the polynomial.*

In this paper,a Blind Signature Scheme is proposed for source privacy. The blind signature schemes with a complexity-based proof of security. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. The blind signature scheme does not have the threshold problem.

I. INTRODUCTION

A network is connected by number of different devices. These different devices providing the different services and used to give different types of systems, in different locations the ability to communicate. The network devices such as routers, hubs, bridges, switches and repeaters.

The whole network system is fully connected through multi-hop communications. Message is tampered in route; it will be detected by the receiver. This method is not effective due to the following reasons: First reason [7] it cannot authenticate messages that are multicast because, if one of the recipients is compromised, the attacker can use the secret key held by the compromised receiver to fake MACs for messages modified by itself to cheat receivers. Secondly, the method only allows end-to-end message authentication en-route forwarding nodes cannot authenticate pass by messages, the intruder may launch denial-of-service attacks by repeatedly modifying messages [5] or injecting false messages to deplete the communication resources of intermediate forwarding nodes.

A secret polynomial [8] based message confirmation plan was introduced. The thought of this plan is like an edge mystery offering, where the edge is controlled by the level of the polynomial. The quantity of messages transmitted is bigger than the limit, the polynomial can be completely recuperated and the framework is totally broken.

II. PREVIOUS WORK

D. Point cheval and J. Stern, "Security Arguments for Digital Signatures" [4] Way to achieve some kind of provable security is to identify concrete cryptography objects such as hash functions with ideal random objects.

M. Bellare and P. Rogawa described "Paradigm for designing efficient protocols"[6] of the random oracle model where all parties have access to a public random oracle provides a bridge between cryptography theory and cryptography practice

Masayuki Abe.et.al [1] "A Secure Three-move Blind Signature Scheme" of the work is security against adaptive and parallel attacks can be proven in the random oracle model either need five data exchanges between the signer and the user

N. Asokan et.al described"Optimistic fair exchange of digital signatures" [2] of the work can also be adapted to exchange encrypted data

R. Rivest.et.al explained [5] "Leak A Secret" in the notion of a ring signature, makes it possible to specify a set of possible signers without revealing which member actually produced the signature.

R. Rivest, et.al "A method for obtaining digital signatures [9] encryption method" presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key.

T.A. ElGamal,"A public key cryptosystem and a signature scheme [10] based on discrete logarithms" are used to a new signature scheme is introduced, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem.

III. PROPOSED WORK

In this paper I have done my work Blind signatures allow a signer to interactively sign messages for users such that the messages are hidden from the signer. Blind signature scheme is mainly used to source privacy. This blind signature scheme enhance the security at three levels by (a) Hiding source node (b) Encrypt the file (c) Generate unique message authentication code(MAC) and signature. Hence it is impossible for an intruder to retrieve the message from intermediate node.

Volume : 5 | Issue : 8 | August 2015 | ISSN - 2249-555X

Fig 1 shows that Security server is responsible for key generation and stores the data. The security server contains the node name, address, port, id, signature, public key and private key. All the details stored to the security server. Every node registered that time retrieve the node details from security server.

Blind Signature Scheme allows a person to get a message signed by another party without revealing any information about the message to the other party. The main purpose of blind signature scheme hides the source node so data is protected to unauthorized person.

Message authentication is an important to the network security. Each and every level provides the unique message authentication code (MAC) and signature created. The data is transferred to node then verify the message authentication code and signature. Every level verification process is occurred.

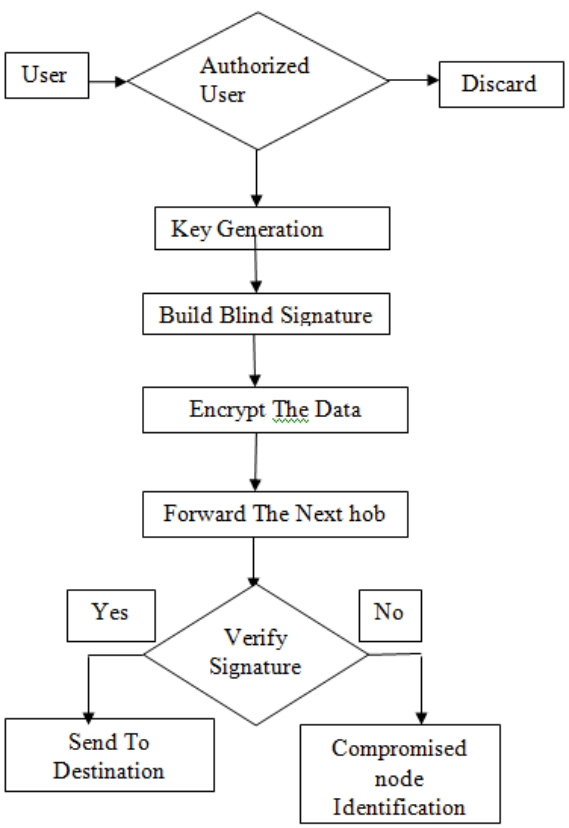

Fig 1 System Mode

A node has been identified as compromised; the SS (Security Server) can remove its public key from its public key list. The public key mainly used to key distribution, authentication and integrity.

The blind signature scheme following some steps

Step 1: Create wireless sensor network
Step 2: Wireless sensor network

Initialization

Step 3: All the nodes are registration
Step 4: Topology configuration
Step 5: Login to the all nodes
Step 6: Browse the file and apply the encryption
Step 7: Active path processing
Step 8: Hide the source node
Step 9: Generate MAC code and signature
Step 10: Forwarder checks the verification and send to the next hop.
Step 11: Finally receiver checks the verification.
Step 12: Verification process completed after decrypt to the file.

IV. Simulation/Experimental Results

Blind Signature Scheme is used to secure level sending the data to one node to another node. If authorized user access the information using this blind signature. Each and every level applies the message authentication process so protecting the information.

Fig 2 Encryption

Figure 2 illustrates a choose file process. In this way encryption process applies to the selected file. The encryption process over and sender ready to send the data. Encryption process mainly used to protecting the information.

Fig 3 Build Active Path

Figure 3 illustrates a sender send to active path request to the ambiguity server. The ambiguity server is providing the active path.

Volume : 5 | Issue : 8 | August 2015 | ISSN - 2249-555X

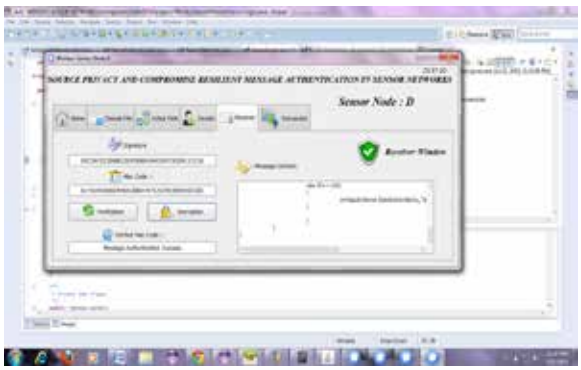

Fig 4 Decryption

Figure 4 shows that a receiver check the verification process.The verified the MAC code then MAC code match and displayed message authentication success and decrypt the data. The original message secure to reach the receiver.

V.CONCLUSION

Blind Signature Scheme is very simple because the source node hide and the information send secure manner. Blind signature scheme working to the multi hob communications so the data is send multiple path. This method access the all path and which one give the minimum cost and that path is take to new active path .This method accessible for the all the virtual graphs. The main purpose of blind signature scheme is cost considerable, message verification, source privacy.

REFERENCE

[1]. Masayuki Abe. A Secure Three-Move Blind Signature Scheme for Polynomially Many Signatures. Advances in Cryptology | Eurocrypt'01, Volume 2045 of Lecture Notes in Computer Science, pages 136{151. Springer-Verlag, 2001. | [2]. N. Asokan, Victor Shoup, and Michael Waidner. Optimistic Fair Exchange of Digital Signatures. Advances in Cryptology | Eurocrypt'98, Volume 1403 of Lecture Notes in Computer Science, pages 591{606. Springer-Verlag, 1998. | [3]. M. Waidner, "Unconditional Sender and Recipient Untraceability in Spite of Active Attacks," Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989. | [4]. D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361- 396, 2000. | [5]. R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Advances in Cryptology (ASIACRYPT), 2001. | [6]. M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigmfor Designing Efficient Protocols," Proc. ACM First Conf. Computer and Comm. Security (CCS '93), pp. 62-73, 1993. [22] "Cryptographic Key Length | [7]. A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, May 2000. | [8]. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009. | [9]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978. | [10]. T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.