International Journal of Science Engineering and Advance Technology

Efficient And Secure Hop-By-Hop Message Authentication And Source Privacy In Wireless Sensor Networks

N. Vijaya Bharatha Lakshmi[1], K.V.S.S. Rama Krishna[2]
[1]M.Tech (CSE), VIGNAN's NIRULA Institute of technology and science for women, A.P., India.
[2]Asst.Professor, Dept. of Computer Science & Engineering, VIGNAN's NIRULA Institute of technology and science for women, A.P., India.

Abstract — security to the data is actually provided by an authentication. Authentication involves a process of confirming an identity. In Wireless sensor networks a lot of message authentication schemes have been developed, based on symmetric-key cryptosystems or public-key cryptosystems. Message authentication is one of the most effective way to prevent illegal and tainted messages from being forwarded in wireless sensor networks (WSNs). For this cause, Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and pliability to node compromise attacks. To address these issues, a Polynomial-based scheme was recently introduced. Though, this scheme and its extensions all have the flaw of a built-in Threshold determined by the degree of the polynomial: when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. In this paper, we suggest a scalable authentication scheme based on *Elliptic Curve Cryptography (ECC) with Schnorr Signcryption.* While enabling intermediate nodes authentication, our proposed scheme solve the threshold problem. In addition, our scheme can also provide message source privacy. Both theoretical analysis and simulation results demonstrate that our proposed scheme is efficient than the polynomial-based approach in terms of computational and communication overhead under comparable security levels.

Keywords — Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless sensor networks (WSNs), distributed algorithm, decentralized control

1. Introduction

Now a Days message authentication plays a key role to prevent the illegal and tainted messages from being forwarded in wireless sensor networks to save the sensor energy. for this reason Various authentication schemes have been developed to give message authenticity and integrity verification for wireless sensor networks (WSNs) [1], [2]. These schemes can mainly be alienated into two categories: public-key based approaches and symmetric-key based approaches very hard to meet also the requirements of complex key management, system usability, resilience and scalability.

An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks. To solve the scalability problem, a secret polynomial based message authentication scheme was introduced in [3]. The thought of this scheme is alike to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. This approach offers information-theoretic security of the shared secret key when the number of messages larger than the threshold. The middle nodes confirm the authenticity of the message through a polynomial assessment. However, when the number of messages larger than the threshold, the polynomial can be fully recovered and the system is totally broken.

We suggested a categorically safe and well-organized source anonymous message authenti-cation (SAMA) scheme based on the schnorr signature on elliptic curves. This scheme is safe next to adaptive chosen message attacks in this model [10].Our system allows the intermediate nodes to validate the message so that all tainted message can be notice and fall to preserve the sensor power. While attain flexible-time authentication compromise resiliency, and source identity protection, our scheme does not have the threshold problem. Both theoretical analysis and simulation results show that our proposed scheme is well-organized than the polynomial-based algorithm under the comparable security levels.

The major contributions of this proposal are the following:

1. We build up a source anonymous message authentication code (SAMAC) on elliptic curves that can offer unqualified source secrecy.
2. We propose a well-organized hop-by-hop message authentication Mechanism for WSNs without the doorsill limitation.

3. We sketch network implementation code on source node solitude protection in WSNs.

4. We recommend an efficient key management framework to make sure isolation of the compromised nodes.

5. We supply widespread simulation results under the Technologies on numerous security levels.

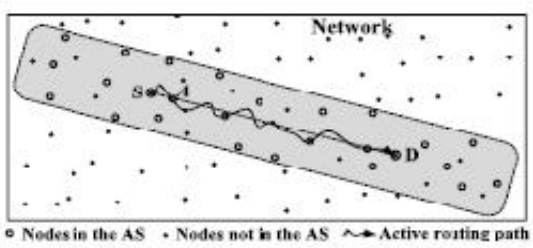

Figure 1 Anonymous set selection in active routing

This is the primary system that gives hop-by-hop node verification without the threshold curb, and has recital better than the symmetric-key based schemes. The dispersed nature of our algorithm creates the scheme appropriate for decentralized networks.

2. PRIMITIVES AND REQUIREMENTS

In this section, we will briefly describe the terminology and the cryptographic techniques that will be used.

Threat Model and Assumptions

We suppose that each sensor node knows its relative site in the sensor area and is able of communicating with its adjacent nodes in a straight line by geographic routing. The entire network is completely connected before outsourcing from side to side multi-hop communications. We take for granted there is a security server (SS) that is accountable for generation, storage and sharing of the safety limit among the network. The compromised nodes will not be clever to make new public keys that can be conventional by the SS and other nodes. Based on the on top of assumptions, this paper considers two types of attacks open by the adversaries: Passive attacks and active attacks. During passive attacks, the opponent could listen in on messages transmitted in the network and carry out traffic analysis. Active attacks can only be start on from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will find all the information stored in the compromised nodes, with the safety parameters of the compromised nodes.

Design Goals:

Message authentication. The message receiver should be capable to authenticate whether a received message is sent by the node that is claimed or by a node in a finicky group. In other words, the adversaries cannot imaginary to be an innocent node and introduce fake messages into the network without being noticed.

Message integrity. The message receiver should be able to bear out whether the message has been modified-route by the adversaries. In other words, the adversaries cannot change the message content without being detected.

Hop-by-hop message authentication. Each forwarder on the routing path should be talented to bear out the legitimacy and truth of the messages upon response.

Identity and location privacy. The adversaries cannot settle on the message sender's ID and location by investigate the message contents or the local traffic.

Node compromise resilience. No topic how many nodes are compromised, the residual nodes can still is safe Efficiency. The scheme should be well-organized in terms of both computational and communication overhead.

Terminology

Privacy is now and then referred to as obscurity. Communication mystery in information management has been discussed in a number of preceding works.

Unidentifiable within a set of subjects. This set is called the AS. Sender anonymity means that a meticulous message is not linkable to any sender, and no message is linkable to a exacting sender. We will establish with the explanation of the categorically protected SAMA.

Algorithm 1 (SAMA). A SAMA consists of the following two algorithms:

Generate (m;Q1,Q2, . … .,Qn). Given a message m and the public keys Q1,Q2, ...,Qn of the AS
S ={A1,A2, . . …,An}, the actual message sender At; $1 < t < n$, produces an anonymous message S(m) using its own private key dt.

Verify S(m). Given a message m and an anonymous message S(m), which includes the public keys of all members in the AS, a verifier can determine whether S(m)is generated by a member in the AS.

The security requirements for SAMA include: Sender ambiguity. The probability that a verifier successfully determines the real sender of the anonymous message is exactly 1=n, where n is the total number of members in the AS.

Unforgeability. An anonymous message scheme is unforgeable if no adversary, given the public keys of all members of the AS and the anonymous messages $m_1,m_2,\ldots,m_n$ adaptively chosen by the adversary, can produce in polynomial time a new valid anonymous message with non-negligible probability.

In this implementation, the user ID and the user public key will be used interchangeably without making any distinctions.

Algorithm 2: Implementation of the New Signcryption Scheme:

Schnorr signcryption scheme produced by the Schnorr signature algorithm[10][11] . it consist of three steps.

Choose parameters:

P: a large prime, q:a prime factor of P-1 and g:is a generator Z_p^* i.e)chosen from integers in [1,…..,p-1] with order q modulo p.

1,Key generation step.

Alice Private key: a number x_a drawn randomly from[1,…..,q-1]

Alice Public key : $y_a = g^{-xa} \bmod p$.

2.Signcryption step**:**

Schnorr suggests that Alice sign a digital document as M, by picking a random from k from[1,…,q-1].and $r = g^k \bmod p$.

Let e=h(M||r) where || denotes concatenation and r is represented as a bit string. H is a cryptographic hash function . $h:\{0,1\}^* \rightarrow Z_p$

Let $s=k+x_a e \bmod q$.

The signature is the pair(e,s)

3.Unsigncryption step:

The procedure for other people to verify alice signature (e,s) on M is straightforward: checking whether

$e_v = h(g^s.y_a^e \bmod p||M)$

then $e_v=h(M||r_v)$

If $e_v=e$ the signcryption is verified and accepted.if it is not equal then reject.

If alice publishes $y_a=g^{xa} \bmod p$, instead of $y_a=g^{-xa} \bmod p$, then s can be defined as $s=k-x_a.e \bmod q$, signature verification is same.

Key management and Node Detection

In our scheme, we assume that there is an SS whose everyday jobs take in public-key storage and distribution in the WSNs. We presume that the SS will by no means be compromised. However, after operation, the sensor node may be detain and compromised by the attackers. Once compromised, all information stored in the sensor node will be available to the attackers. We added assume that the compromised node will not be bright to form new public keys that can be customary by the SS. For competence, each public key will have a short uniqueness. The length of the distinctiveness is based on the scale of the WSNs.

As the SAMA system assurance that the message honesty is untampered, when a bad or empty message is conventional by the sink node, the source node is sight as cooperation. If the compromised source node only broadcast one message, it would be very hard for the node to be recognized without extra network traffic information.

If the compromised nodes repetitively use the same AS, it makes transfer examination of the compromised nodes reasonable, which will enlarge the likelihood for the compromised nodes to be notorious and captured. When a node has been identified as conciliation, the SS can eliminate its public key from its public key list. It can also screen the node's short characteristics to the entire sensor domain so that any sensor node that uses the stored public key for an AS selection can keep posted its key list. Once the public key of a node has been detached from the public key list, and/or broadcasted, any message with the AS hold the compromised node should be fall without any procedure in arrange to put aside the valuable sensor power.

3. RELATED WORK

In [1], [2], symmetric key and hash based authentication, schemes were proposed for WSNs. each symmetric authentication key is shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. Therefore, these schemes are not resilient to node compromise attacks. To address these issues a secret polynomial based message Authentication scheme was introduced in [3]. This idea offers information-theoretic defense with ideas analogous to a threshold secret sharing, where the threshold is resolute by the degree of the polynomial. When the number of messages transmitted is below threshold, the scheme enable the intermediate node to confirm the genuineness of the message through polynomial evaluation. On the other hand, when the number of messages transmitted is larger than the threshold, the polynomial can be entirely recovered and the system is totally broken. To add to the threshold and the difficulty for the intruder to rebuild the secret polynomial, random noise, also called a perturbation factor, was added to the polynomial in [4] to frustrate the adversary from calculate the coefficient of the polynomial. Though, the added perturbation factor can be wholly detached using error-correcting code techniques [6]. For the public-key based approach, each message is transmitted along with the digital signature of the message generated by using the sender's private key.

4. PROPOSED MESSAGE AUTHENTICATION ON ELLIPTIC CURVES

We recommend a categorically safe and efficient SAMA. The major thought is that for each message m to be released, the message sender, or the sending node, generates a basis anonymous message authenticator for the message m. The generation is based on the Schonnr signcryption scheme on elliptic curves. For a ring signature, each ring member is required to compute a signature for all other members in the AS. In our format, the entire SAMA to be verified through single equation with out individually verifying the signature

Proposed Schonnr signcryption Scheme on Elliptic Curves

An elliptic curve E is defined by an equation of the form: E: $y^2=x^3+ax+b \bmod p$

Where a,b ϵ F_p. The set $E(F_p)$ consists of all points $(x,y) \epsilon F_p$ on the Curve, to gather with a Special point O, called the point at infinity.

Let p be the point on the $E(F_p)$. Alice can select a random integer $d_a \epsilon [1,N-1]$ as his private key. Then he can compute his public key Q_a from $Q_a=d_a*p$.

Signature generation step: Alice to sign the message m,[from algorithm2 signcryption step is applied] the signature pair(e,s) is generated then it can be transferred.

Signature verification step: for Bob to authenticate alice's signature, then he must have copy the public key Q_a and checks that Q_a is lies on the curve or not. Then only he should verify the signature.[from algorithm 2 unsigncryption step is applied] the signature is valid based on the verification step, then accepts otherwise rejects.

Proposed SAMA Scheme on Elliptic Curves

An elliptic curve E is defined by an equation of the form: E: $y^2=x^3+ax+b \bmod p$.

Where a,b ϵ F_p. The set $E(F_p)$ consists of all points $(x,y) \epsilon F_p$ on the Curve.

Authentication generation [from algorithm1 generation step] then produces a anonymous message S(m) is transferred to different nodes.

Verification step: Bob to verify an alleged SAMA of S(m) , he must have a copy of the public keys Q1, Q2 ….....,Qn. Then he checks Q_i ,i=1,…,n lies on the curve or not . Then only he should verify the signature.[from algorithm 2 verification step is applied]the message is valid based on the verification step then accepts otherwise rejects.

Performance analysis step based on theoretical analysis we will evaluate our proposed schonnr signcryption scheme with the MES described in [10], [11] the computational cost is less in Schonnr signcryption when compare to MES. A fair comparison between them is shown [11].

5. CONCLUSION

We projected a novel and efficient SAMA based on ECC. Even as make sure message sender privacy, SAMA can be practical to any message to provide message content authenticity. To provide hop-by-hop message authentication without the weak spot of the built-in threshold of the bivariate polynomial-based scheme, we then planned a hop-by-hop message authentication scheme based on the SAMA and Schnorr signcryption. When practical to WSNs with fixed sink nodes, we also converse possible practice for compromised node discovery. Both theoretical and simulation results show that, in similar scenarios, our proposed system is more well-organized than the bivariate polynomial based scheme and MES in terms of computational cost and communication overhead, message delay energy consumption, delivery ratio, and memory use. the following task seem interesting in future research: Designing schemes to support dynamic group member management in the sense that group member can join or leave the group efficiently and dynamically.

REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, Mar. 2004.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By- Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr. 1992.

[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[5] 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.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[7] 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.

[8] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387-398, 1996.

[9] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[10] Journal of Software Engineering and Applications, 2012, 5, 102-108 .Published Online Feb 2012. (http://www.SciRP.org/journal/jsea)
" Combining Public Key Encryption with Schnorr Digital Signature". Laura Savu Department of Information Security, Faculty of Mathematics and Computer Science, University of Bucharest, Bucharest, Romania.

[11]Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost (En-cryption)," Full Version,2011. http://www.sis.uncc.edu/yzheng/papers/

[12] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.

[13] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[14] A. Pfitzmann and M. Waidner, "Networks without User Observability—
Design Options.," Proc. Advances in Cryptology (EUROCRYPT),vol. 219, pp. 245-253, 1985.

[15] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," In: G. Brassard, Ed., *Advances in Cryptol-ogy—Crypto*'89, *Lecture Notes in Computer Science No* 435, Springer-Verlag, 1990. pp. 239-252.