International Journal of Research in Advent Technology, Vol.5, No.4, April 2017
E-ISSN: 2321-9637
*Available onlin*e at www.ijrat.org

Message Authentication & Source Privacy Using Hop by Hop in WSN's

Pratik A. Naringe, Apurva P. Tidke[2], Samruddhi D. Thakare[3], Vinit V. Pande[4],Sanjana S. Puri[5], Sunita M. Wadaskar
Department of Electronics & Telecommunication Engineering,
Jagadambha College Of Engineering And Technology, Yavatmal.
Email: pnaringe@gmail.com, ptapurva22@gmail.com[2], samruddhithakare3@gmail.com, vinitpande3@gmail.com, sanjanappuri@gmail.com, sunitawadaskar16@gmail.com

Abstract: Message authentication is one of the most efficient way to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, predicated on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the inhibitions of high computational and communication overhead in integration to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-predicated scheme was recently introduced. However, this scheme and its extensions all have the impuissance of a built-in threshold determined by the degree of the polynomial: when the number of messages transmitted is more sizably voluminous than this threshold, the adversaries can planarity in saturate the polynomial. In this project, propose a scalable authentication scheme predicated on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme sanctions any node to transmit an illimitable number of messages without suffering the threshold quandary. In integration, our scheme can withal provide message source privacy. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial- predicated approach in terms of computational and communication overhead under commensurable security levels while providing message source privacy.

Keywords: Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless sensor network (WSNs)

I. INTRODUCTION

Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to preserve the precious sensor energy. For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs). These schemes can largely be divided into two categories: public-key predicated approaches and symmetric key predicated approaches. The symmetric-key predicated approach requires involute key management, lacks of scalability, and is not resilient to astronomically immense numbers of node compromise attacks since the message sender and the receiver have to apportion a secret key. The shared key is utilized by the sender to engender a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In integration, this method does not work in multicast networks. To solve the scalability quandary, a secret polynomial predicated message authentication scheme was introduced in. The conception of this scheme is kindred to a threshold secret sharing, where the threshold is tenacious by the degree of the polynomial. This approach offers the information- theoretic security of the shared secret key when the number of messages transmitted is less than the threshold. The intermediate nodes verify the authenticity of the message through a polynomial evaluation. However, when the number of messages transmitted is more sizably voluminous than the threshold, the polynomial can be plenarily recuperated and the system is thoroughly broken. An alternative solution was proposed in to thwart the intruder from recuperating the polynomial by computing the coefficients of the polynomial. The conception is to integrate a desultory noise, withal called a perturbation

factor, to the polynomial so that the coefficients of the polynomial cannot be facilely solved. However, a recent study shows that the arbitrary noise can be thoroughly abstracted from the polynomial utilizing error-redressing code techniques. For the public-key predicated approach, each message is transmitted along with the digital signature of the message engendered utilizing the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message utilizing the sender's public key. One of the constraints of the public-key predicated scheme is the high computational overhead. The recent progress on elliptic curve cryptography (ECC) shows that the public key schemes can be more salutary in terms of computational involution, recollection utilization, and security resilience, since public-key predicated approaches have a simple and clean key management. In this paper, we propose an unconditionally secure and efficient source incognito message authentication (SAMA) scheme predicated on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive culled-message attacks in the desultory oracle model. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor puissance. While achieving compromise resiliency, flexible-time authentication and source identity auspice, our scheme does not have the threshold quandary. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-predicated algorithms under commensurable security levels. The major contributions of this paper are the following:

We develop a source incognito message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. We offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold circumscription. We devise network implementation criteria on source node privacy auspice in WSNs. We propose an efficient key management framework to ascertain isolation of the compromised nodes. We provide extensive simulation results under ns-2 and TelosB on multiple security levels. To the best of our erudition, this is the first scheme that provides hop-by hop node authentication without the threshold inhibition, and has performance better than the symmetric-key predicated schemes. The distributed nature of our algorithm makes the scheme felicitous for decentralized networks.

II. TERMINOLOGY AND PRELIMINARY

We will briefly describe the terminology and the cryptographic implements that will be utilized in this.

2.1 Terminology: Privacy is sometimes referred to as anonymity. Communication anonymity in information management has been discussed in a number of precedent works. It generally refers to the state of being unidentifiable within a set of subjects. This set is called the AS. Sender anonymity designates that a particular message is not linkable to any sender, and no message is linkable to a particular sender. We will commence with the definition of the unconditionally secure SAMA. A SAMA consists of the following two algorithms: Engender (m; Q1; Q2; . . . ; Qn). Given a message m and the public keys Q1; Q2; . . . ; Qn of the AS S ¼ fA1; A2; . . . ; Ang, the genuine message sender At; 1 _ t _ n, engenders an innominate message Some utilizing its own private key dt. At; 1_ t _ n, engenders an incognito message Some utilizing its own private key dt. Given a message m and an innominate message Same, which includes the public keys of all members in the AS, a verifier can determine whether Some is engendered by a member in the AS. The security requisites for SAMA include: Sender ambiguity. The probability that a verifier prosperously determines the authentic sender of the incognito message is precisely 1=n, where n is the total number of members in the AS. Unforgetability. An incognito message scheme is unforgetable if no adversary, given the public keys of all members of the AS and the innominate messages m1; m2; . . . ; mn adaptively culled by the adversary, can engender in polynomial time an incipient valid anonymous message with non-negligible probability.

III. RELATED WORK

In, symmetric key and hash predicated authentication schemes were proposed for WSNs. In these schemes, each symmetric authentication key is shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. Ergo, these schemes are not resilient to node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes. These schemes, including TESLA and its variants, can withal provide message sender authentication. However, this scheme requires initial time synchronization, which is not facile to be implemented on a colossal scale WSNs. In integration, they additionally introduce the delay in message authentication, and the delay increases as the network scale-up. A secret polynomial predicated

message authentication scheme was introduced in. This scheme offers information- theoretic security with conceptions homogeneous to a threshold secret sharing, where the threshold is resolute by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when the number of messages transmitted is more astronomically immense than the threshold, the polynomial can be planarity recuperated and the system is thoroughly broken. To increment the threshold and the intricacy for the intruder to reconstruct the secret polynomial, a desultory noise, withal called a perturbation the factor was integrated to the polynomial in to thwart the adversary from computing the coefficient of the polynomial. However, the integrated perturbation factor can be planarity abstracted utilizing error-rectifying code techniques. For the public-key predicated approach, each message is transmitted along with the digital signature of the message engendered utilizing the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message utilizing the sender's public key. The recent progress on ECC shows that the public-key schemes can be more benign in terms of recollection utilization, message involution, and security resilience since public-key predicated approaches have a simple and clean key management. The subsisting incognito communication protocols are largely stemmed from either mix net or DC-net. A mix net provides anonymity via packet re-shuffling through a set of commix servers (with at least one being trusted). In a mix net, a sender encrypts an outgoing message, and the ID of the recipient, utilizing the public key of the commix. The commix accumulates a batch of encrypted messages, decrypts and reorders these messages, and forwards them to the recipients. Since mix net-like protocols rely on the statistical properties of the background traffic, they cannot provide provable anonymity.

IV. PROBLEM STATEMENT

1. Existing Model: The public-key predicated approach, each message is transmitted along with the digital signature of the message engendered utilizing the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message utilizing the sender's public key. One of the inhibitions of the public-key predicated scheme is the high computational overhead. Computational intricacy, recollection utilization, and security resilience, since public-key predicated approaches have a simple and clean key management. Disadvantages: High computational and communication overhead. Lack of scalability and resilience to node compromise attacks. Polynomial-predicated scheme has the impotency of a built-in threshold determined by the degree of the polynomial.

2. Proposed System: We propose an unconditionally secure and efficient SAMA. The main conception is that for each message m to be relinquished, the message sender, or the sending node, engenders a source incognito message authenticator for the message m. The generation is predicated on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS. In our scheme, the entire SAMA generation requires only three steps, which link all nonsenders and the message sender to the SAMA homogeneous. In additament, our design enables the SAMA to be verified through a single equation without individually verifying the signatures. Advantages: A novel and efficient SAMA predicated on ECC. While ascertaining message sender privacy, SAMA can be applied to any message to provide message content authenticity. To provide hop-by-hop message authentication without the impuissance of the built- in a threshold of the polynomial based scheme, we then proposed a hop-by-hop message authentication scheme predicated on the SAMA.When applied to WSNs with fine- tuned sink nodes, we withal discussed possible techniques for compromised node identification.

V. KEY MANAGEMENT AND DEFINITION

In our scheme, we surmise that there is an SS whose responsibilities include public-key storage and distribution in the WSNs. We surmise that the SS will never be compromised. However, after deployment, the sensor node may be captured and compromised by the assailants. Once compromised, all information stored in the sensor node will be accessible to the assailers. We further postulate that the compromised node will not be able to engender incipient public keys that can be accepted by the SS. For efficiency, each public key will have a short identity. The length of the identity is predicated on the scale of the WSNs.

VI. SYMMETRIC KEY AND CRYPTOSYSTEM MESSAGE

Authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to preserve the precious sensor energy. For this reason, many authentication schemes have been proposed in the literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs). These schemes can largely be divided into two categories: public-key predicated approaches and symmetric keys predicated approaches. The symmetric-key predicated approach requires involute key management, lacks scalability, and is not resilient to astronomically immense numbers of node compromise attacks since the message sender and the receiver have to apportion a secret key. The shared key is utilized by the sender to engender a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In additament, this method does not work in multicast networks.

VII. PUBLIC-KEY CRYPTOSYSTEM

For the public-key predicated approach, each message is transmitted along with the digital signature of the message engendered utilizing the senders private key. Every intermediate forwarder and the final receiver can authenticate the message utilizing the senders public key. One of the constraints of the public-key predicated scheme is the high computational overhead. The recent progress on elliptic curve cryptography (ECC) shows that the public key schemes can be more propitious in terms of computational involution, recollection utilization, and security resilience since public-key predicated approaches have a simple and clean key management.

VIII. HOP-BY-HOP AUTHENTICATION

Message authentication: The message receiver should be able to verify whether a received message is sent by the node that is claimed, or by a node in a particular group. In other words, the adversaries cannot pretend to be an irreprehensible node and inject fake messages into the network without being detected.

Message integrity: The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected. Hop-by-hop message authentication every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.Hop-by-hop message authentication every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

Identity and location privacy: The adversaries cannot determine the message senders ID and location by analyzing the message contents or the local traffic. Efficiency The scheme should be efficient in terms of both computational and communication overhead.

IX. ANALYSIS AND EXPERIMENTAL RESULTS

In this section, we will evaluate our proposed authentication scheme through both theoretical analysis and simulation demonstrations. We will compare our proposed scheme with the bivariate polynomial-predicated symmetric-key scheme described. A fair comparison between our proposed scheme and the scheme proposed in should be performed with n ¼ The congruous cull of an AS plays a key role in message source privacy, since the genuine message source node will be obnubilated in the AS. In this section, we will discuss techniques that can avert the adversaries from tracking the message source through the AS analysis in amalgamation with local traffic analysis. Afore a message is transmitted, the message source node culls an AS from the public key list in the SS as its cull. This set should include itself, together with some other nodes. When an adversary receives a message, he can possibly find the direction of the anterior hop, or even the authentic node of the antecedent hop. However, the adversary is unable to distinguish whether the anterior node is the genuine source node or simply a forwarder node if the adversary is unable to monitor the traffic of the anterior hop. Ergo the cull of the AS should engender adequate diversity so that it is infeasible for the adversary to find the message source predicated on the cull of the AS itself. Some rudimentary criteria for the cull of the AS can be described as follows: To provide message source privacy, the message source needs to cull the AS to include nodes from all directions of the source node. In particular, the AS should include nodes from the antithesis direction of the successor node. In this way, even the immediate successor node will not be able to distinguish the message source node from the forwarder predicated on the message that it receives. Though the message source node can cull any node in the AS, some nodes in the AS may not be

able to integrate any ambiguity to the message source node. For instance, the nodes that are ostensibly infeasible or very unlikely to be included in the AS predicated on the geographic routing. Ergo, these nodes are not congruous candidates for the AS. They should be omitted from the AS for energy efficiency. To balance the source privacy and efficiency, we should endeavor to cull the nodes to be within a predefined distance range from the routing path. We recommend culling an AS from the nodes in a band that covers the active routing path. However, the ASdoes not have to include all the nodes in the routing path. The AS does not have to include all nodes in that range, nor does it have to include all the nodes in the active routing path. In fact, if all nodes are included in the AS, then this may avail the adversary to identify the possible routing path and find the source node.

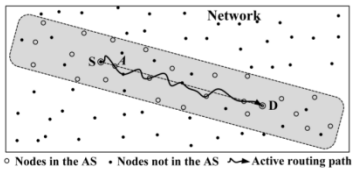
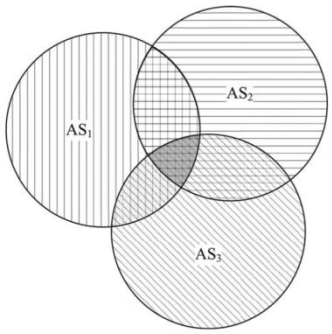


Fig1.Anonymous set selection in active routing.

As an example, suppose we operate to transmit a packet from source node S to destination node D in Fig. 1. We cull the AS to include only nodes marked with, while nodes marked as will not be included in the AS. Of all these nodes, some of them are on the active routing path while others are not. However, all these nodes are located within the shaded band area circumventing the active routing path. Suppose node A is compromised unless node A collaborates with other nodes and can plenarily monitor the traffic of the source node S, it will not be able to determine whether S is the source node, or simply a forwarder. A kindred analysis is withal true for other nodes. Any node in the active routing path can verify the contents‟ authenticity and integrity. However, anybody who receives a packet in the transmission can possibly omit some of the nodes in the WSNs as the possible source node. The inclusion of these nodes in the AS will not increment the source privacy. Nevertheless, the more the nodes included in the AS are, the higher the energy cost will be. Consequently, the cull of the AS has to be done with care so that the energy cost and the source privacy can both be optimized. In additament, to balance the potency consumption between authenticity and integrity verification, and the possibility that corrupted messages are being forwarded, the verification accommodation may not have to take place in every hop; instead, it may be configured to take place in every other hop, for instance. As a special scenario, we postulate that all sensor information will be distributed to a sink node, which can be collocated with the SS. As described in Section 5, when a message is received by the sink node, the message source is obnubilated in an AS. Since the SAMA scheme guarantees that the message integrity is untampered, when a deplorable or frivolous message is received by the sink node, the source node is viewed as compromised. If the compromised source node only transmits one message, it would be very arduous for the node to be identified without supplemental network traffic information. When a compromised node transmits more than one message, the sink node can narrow the possible compromised nodes down to a minutely diminutive set. As shown in Fig. 2, we utilize the circle to represent an AS. When only one message is transmitted, the sink node can only obtain the information that the source node will be in a set, verbalize AS1. When the compromised source node transmits two messages, the sink node will be able to narrow the source node down to the set with both vertical lines and horizontal lines. When the compromised source node transmits three messages, the source node will be further narrowed down to the shaded area. Consequently, if the sink node keeps tracking the compromised message, there is a high probability that the compromised node can be isolated.



. Fig. 2.Compromised node detection.

\

X. OUTPUT GRAPHS

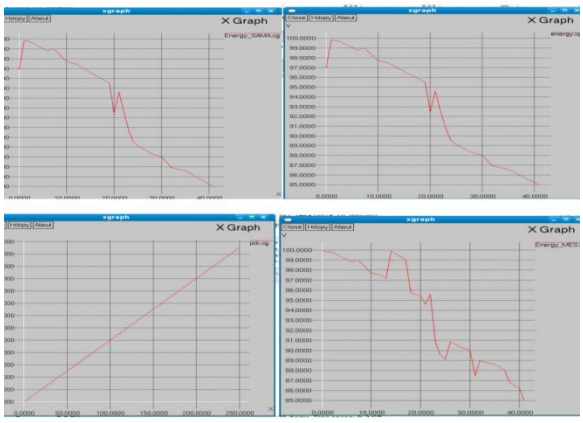


fig:output graphs.

XI. CONCLUSION

In this project, we first proposed a novel and efficient SAMA predicated on ECC. While ascertaining message sender privacy, SAMA can be applied to any message to provide message content authenticity. To provide hop-by-hop message authentication without the impotency of the built-in the threshold of the polynomial-predicated scheme, we then proposed a hop-by-hop message authentication scheme predicated on the SAMA. When applied to WSNs with fine-tuned sink nodes, we withal discussed possible techniques for compromised node identification. We compared our proposed scheme with the bivariate polynomial-predicated scheme through simulations utilizing ns-2 and TelosB. Both theoretical and simulation results show that incommensurable scenarios, our proposed scheme is more efficient than the bivariate polynomial-predicated scheme in terms of computational overhead, energy consumption, distribution ratio, message delay, and recollection consumption

REFERENCES

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

[2]"Cryptographic Key Length Recommendation," http://www.keylength.com/en/3/, 2013.

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

[4] 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. 1118, 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.