ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

High Privacy through Hop-by-Hop Message Authentication in Wireless Sensor Networks

V.Gayatri[1], Ch.Venkateswarlu[2], T.Venkatapathi[2]

Associate Professor, Dept. of CSE, Geethanjali Institute of Science & Technology, Nellore, AP, India

M.Tech Student, Dept. of CSE, Geethanjali Institute of Science & Technology, Nellore, AP, India

M.Tech Student, Dept. of CSE, Geethanjali Institute of Science & Technology, Nellore, AP, India

ABSTRACT: Message authentication is one of the most effective solutions to thwart unauthorized as well as corrupted messages via being forwarded inside wireless sensor networks (WSNs). For this particular reason, many message authentication schemes have been developed, based about either symmetric-key cryptosystems as well as public-key cryptosystems. Many, however, have the disadvantages of high computational as well as communication overhead as well as need of scalability as well as resilience to node skimp attacks. To address these issues, a polynomial-based scheme was recently introduced. In proposed system concentrates on providing high privacy to the message authentication. In addition to hop-by-hop message authentication key exchange mechanism is enable through deffiee helmen key exchange algorithm the source node encrypts the data after receiver the data it needs a private key for decrypting the data. So the receiver request key server to produce a private key. The key server authenticates the receiver access through key authentication. It is very hard for malicious node to get a key from key server.

KEYWORDS*:* Providing Privacy, Hop-By-Hop, Source Anonymous Message Authentication (SAMA),Elliptic Contour Cryptography (ECC), Wireless Sensor Networks.

I. INTRODUCTION

Message authentication is among the most effective solutions to thwart unauthorized in addition to corrupted messages from being forwarded with wireless sensor communities (WSNs). For this particular reason, many authentication schemes are proposed in literature to supply message authenticity in addition to integrity verification intended for wireless sensor communities (WSNs) [1]–[5]. These schemes can largely be divided in two categories: public-key centered approaches and symmetric-key centered approaches.

The symmetric-key centered approach necessitates amalgamated key management, lacks of scalability, and is definitely not flexible to many node compromise attacks because message sender plus the receiver have to share with you a secret essential. The shared essential is handled from the sender to produce a message authentication code (MAC) for every transmitted message. Nonetheless, for this process the authenticity and integrity of the message can simply be confirmed from the node with your shared secret essential, which is typically shared by a gaggle of sensor nodes. An intruder can compromise the real key by incarcerating 1 sensor node. Moreover, this method is not useful in multicast communities. For the public-key centered method, each message is transmitted along with the digital signature of the message produced using the sender's private essential. Every intermediate forwarder plus the final receiver may authenticate the message using the sender's public essential [6], [7]. One of the restrictions of the public key based method could be the high computational cost.

Threat Model and Assumptions:

The wireless sensor communities are implicit to be able to consist of a ton of sensor nodes. The assumption is that each sensor node understands its relative location from the sensor domain and is competent of communicating featuring a neighboring nodes specifically using geographic course-plotting. The entire system is fully attached through multi-hop marketing communications. It is assumed that there is a security server (SS) which is liable for era, storage and distribution of the security parameters one of the network. This server will in no way be compromised. Nonetheless,

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

after deployment, the sensor nodes could be compromised and seized by attackers. The moment compromised, all data stored from the sensor nodes can be acquired by the opponents. The compromised nodes might be reprogrammed and completely managed from the attackers.

To resolve the scalability difficulty, a secret polynomial centered message authentication plan was introduced with [3]. The idea of this scheme is related to a threshold magic formula sharing, where the threshold relies on the degree of the polynomial. This approach delivers information-theoretic security of the shared secret key when the quantity of messages transmitted is under the threshold. The intermediate nodes authenticate the Authenticity of the message through a new polynomial evaluation. Nonetheless, when the volume of messages transmitted is bigger than the threshold, the polynomial might be fully recovered plus the system is totally broken. An alternative solution was proposed with [4] to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is usually to add a randomly noise, also known as a perturbation factor, to the polynomial so the coefficients of the polynomial can't be easily solved. None the less, a recent study demonstrates the random noise might be completely removed from the polynomial using error-correcting signal techniques [6]. To the public-key based technique, each message is transmitted along with the digital signature of the message generated using the sender's private essential. Every intermediate forwarder plus the final receiver may authenticate the message using the sender's public essential [7], [8]. One of the limitations of your publickey based scheme could be the high computational cost. The recent advance on elliptic contour cryptography (ECC) demonstrates the public-key schemes might be more advantageous with regards to computational complexity, recollection usage, and safety measures resilience, since public-key based approaches possess a simple and clean key management [9].

In this particular paper, we propose the unconditionally secure in addition to efficient source unknown message authentication (SAMA)scheme based on the optimal modified ElGamal signature(MES) plan on elliptic curves. This MES plan is secure against adaptive chosen-message attacks from the random oracle design [10].

However, the compromised nodes will struggle to produce new public keys that could be accepted by the SS along with other nodes. Two forms of possible attacks launched from the adversaries are:

• ***Passive attacks:*** By passive attacks, the adversaries can snoop on messages transmitted from the network and do traffic analysis.

• *Active attacks:* Active attacks may only be commenced from the compromised sensor nodes. In the event the sensor nodes are generally compromised, the adversaries will gain every one of the data stored from the compromised nodes, such as security. Parameters of the compromised nodes. The adversaries can transform the contents of the messages, and introduce their very own messages. An authentication protocol need to be resistant to node skimp on by allowing protected key management. The protocol may provide an integrated key-rotation mechanism or allow for key rotation by an external component.

II. BACKGROUND OR RELATED WORK

In [1], [2], symmetric key and hash based 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. Therefore, these schemes are not resilient to node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes. These schemes, including TESLA [5] and its variants, can also provide message sender authentication. However, this scheme requires initial time synchronization, which is not easy to be implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up. A secret polynomial based message authentication scheme was introduced in [3]. This scheme offers information-theoretic security with ideas similar to a threshold secret sharing, where the threshold is determined 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 larger than the threshold, the polynomial can be fully recovered and the system is completely broken. To increase the threshold and the complexity for the intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was added to the polynomial in [4] to thwart the adversary from computing the coefficient of the polynomial. However, the added perturbation factor can be completely removed 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 using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. The recent progress on ECC shows

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience, since public-key based approaches have a simple and clean key management [9]. The existing anonymous communication protocols are largely stemmed from either mixnet [11] or DC-net [12]. A mixnet provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). In a mixnet, a sender encrypts an outgoing message, and the ID of the recipient, using the public key of the mix. The mix accumulates a batch of encrypted messages, decrypts and reorders these messages, and forwards them to the recipients. Since mixnet-like protocols rely on the statistical properties of the background traffic, they cannot provide provable anonymity. DC-net [12], [16] is an anonymous multi-party computation scheme. Some pairs of the participants are required to share secret keys. DC-net provides perfect (information-theoretic) sender anonymity without requiring trusted servers. However, in DC-net, only one user can send at a time, so it takes additional bandwidth to handle collision and contention.

III. COTRIBUTION

The major contributions of this paper are the following:

1. We develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity.
2. We offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation.
3. We devise network implementation criteria on source node privacy protection in WSNs.
4. We propose an efficient key management framework to ensure isolation of the compromised nodes.
5. We provide extensive simulation results under ns-2 and TelosB on multiple security levels.

To the best of our knowledge, this is the first scheme that provides hop-by-hop node authentication without the threshold limitation, and has performance better than the symmetric-key based schemes. The distributed nature of our algorithm makes the scheme suitable for decentralized networks.

IV. PROPOSED METHODOLOGY

In this section, we propose an unconditionally secure and efficient SAMA. The main idea is that for each message mto be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based 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 non-senders and the message sender to the SAMA alike. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

Our proposed authentication scheme aims at achieving the following goals:

1.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 innocent node and inject fake messages into the network without being detected.

2.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 [1].

3.Identity and location privacy:

The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic [3].

4. Efficiency:

The scheme should be efficient in terms of mutually computational and communication overhead [15]. In proposed system concentrates on providing high privacy to the message authentication. In addition to hop-by-hop message authentication key exchange mechanism is enable through deffiee helmen key exchange algorithm the source node encrypts the data after receiver the data it needs a private key for decrypting the data. So the receiver request key server to produce a private key. The key server authenticates the receiver access through key authentication. It is very hard for malicious node to get a key from key server.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

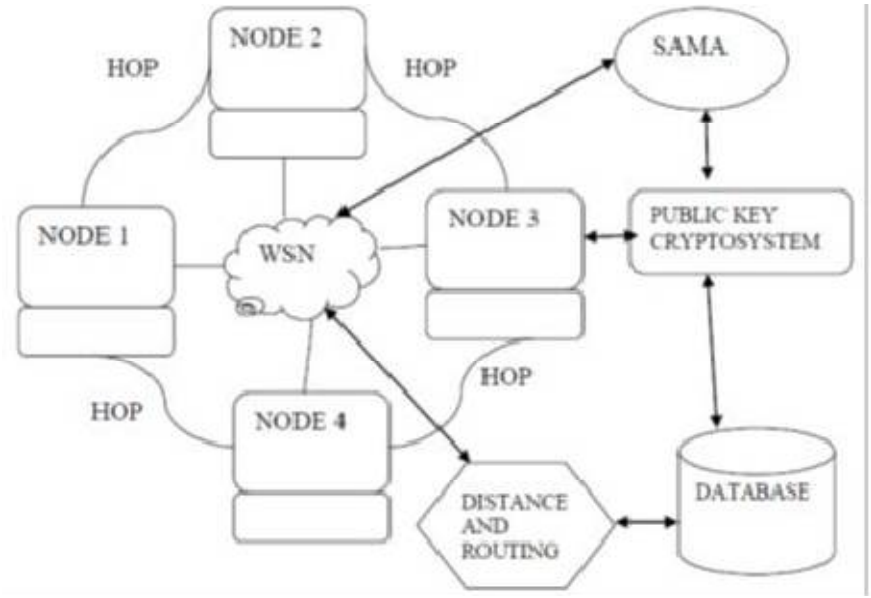


Fig: Hop by Hop Message Authentication and Source Privacy in Wireless Sensor Networks.

In wireless sensor network provides on high privacy to the message authentication. While enabling intermediate nodes message authentication scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. We develop a source anonymous authentication code (SAMAC) an elliptical curve that can be provide unconditional source anonymity through hop-by-hop message authentication process.

V. EXPERIMENTAL RESULTS

In this section, we implement the bivariate polynomial based scheme and our proposed scheme in a real world comparison. The comparison is based on comparable security levels. The implementation in [4] was carried out on Mica2 platform, which is 8 MHz, while our implementation is carried out on Telosb platform, which is 4 MHz. We first provide simulation in Table 1 to compare and justify our parameter selections. From the table, we can see that our result is comparable with the original paper. This justifies that the performance comparisons between our scheme and the algorithm proposed in [4] using different parameters are consistent and reasonable.

TABLE 1: Performance Comparison of the Bivariate Polynomial-Based Scheme in Two Different Scenarios: (a) The Original Implementation under 8 MHz Mica2 Platform, and (b) Our Implementation under 4 MHz Telosb

(a). Original implementation [4]							
$d_x, d_y = 3$				$d_x, d_y = 4$			
ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)	ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)
14.78	1938	5.8	57.89	15.04	2211	7.59	70.8
(b). Our implementation							
$d_x, d_y = 3$				$d_x, d_y = 4$			
ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)	ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)
13.61	1938	9	108	13.65	2302	11.73	126.93

Table 2 shows the process time of our scheme and the bivariate polynomial-based scheme for both authentication generation and verification. In the simulations, we assume that the key length of our scheme is 2l.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

From the table, we have the following findings:

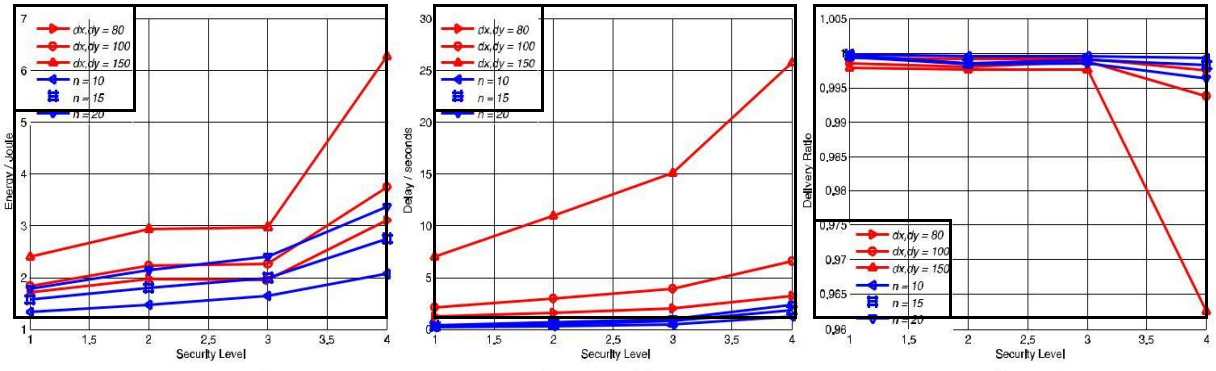
- For the bivariate polynomial-based scheme, the authentication generation time is much longer than the verifying time; while for our proposed scheme, the verifying time is about half of the authenticationgeneration time, except when n= 1, the generation time is shorter than the verification time.
- Comparing bivariate polynomial-based scheme with our proposed scheme for n= 1, we find that the gen-eration time of our scheme is less than 5 percent of the bivariate polynomial-based scheme for all d_x; d_y, but the verifying time is slightly longer when d_x; d_y is less than 100. When d_x; d_y is longer than 150, the verifying times of the two schemes are comparable.
- The memory consumption of our proposed scheme is slightly less than the bivariate polynomial-based scheme in all scenarios.
- For our proposed scheme, to provide source privacy, the cost of generation time and verifying time increase linearly with n.

TABLE 2: Process Time (s) for the Two Schemes (16-bit, 4 MHz TelosB Mote)

	Polynomial-based approach						Proposed approach							
	$d_x, d_y = 80$		$d_x, d_y = 100$		$d_x, d_y = 150$		$n = 1$		$n = 10$		$n = 15$		$n = 20$	
	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify
$l = 24$	9.31	0.25	14.45	0.31	31.95	0.46	0.24	0.53	4.24	2.39	6.16	3.51	8.38	4.44
$l = 32$	12.95	0.33	20.05	0.41	44.60	0.62	0.34	0.80	5.99	3.32	8.92	5.05	12.19	6.42
$l = 40$	13.32	0.35	20.57	0.44	45.73	0.65	0.46	1.05	8.03	4.44	11.94	6.71	16.18	8.50
$l = 64$	21.75	0.57	33.64	0.71	74.85	1.06	1.18	1.77	20.53	11.03	30.12	16.41	41.44	21.10
$l = 80$	26.40	0.70	41.03	0.88	90.86	1.30	1.46	2.22	25.58	13.90	37.66	20.96	50.96	26.18

The simulation results in Figs. 3a and 3b demonstrate that our proposed scheme has a much lower energy consumption and message transmission delay. These simulations were carried out in ns-2 on RedHat Linux system. The security levels 1, 2, 3, 4 correspond to symmetric key sizes 24, 32, 40, and 64 bits, and elliptic curves key size 48, 64, 80, and 128 bits, respectively.

We also conduct simulations to compare the delivery ratios using ns-2 on RedHat Linux system. The results show that our scheme is slightly better than the bivariate polynomial-based scheme in delivery ratio. The results are given in Fig. 3c.



(a) Energy consumption (b) Message delay (c) Delivery ratio

Fig. 3. Performance comparison of our proposed scheme and bivariate polynomial-based scheme.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Our simulation on memory consumption derived in TelosB, sees Table 3, and shows the overall memory consumption for bivariate polynomial-based scheme is at least five times larger than our proposed scheme.

TABLE 3: Memory (KB) for the Two Schemes (TelosB) (F Stands for Flash Memory)

	Polynomial-based approach									**Proposed approach**											
	$d_x, d_y = 80$			$d_x, d_y = 100$			$d_x, d_y = 150$			$n = 1$			$n = 10$			$n = 15$			$n = 20$		
	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F
$l = 24$	21	3	26	21	4	40	26	4	90	21	1	0	21	2	0	21	2	0	21	2	0
$l = 32$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	2	0
$l = 40$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	3	0
$l = 64$	21	6	64	21	7	100	26	9	225	21	2	0	22	3	0	22	3	0	22	3	0
$l = 80$	21	7	77	21	8	120	26	10	270	20	2	0	21	3	0	21	3	0	21	4	0

VI. CONCLUSION

In order to secure your communication message authentication in authentication only one can achieve great plant the proper tree of authenticity. This paper is in order to investigate the different techniques available in message Authentication. In future to develop the new efficient authentication scheme using the elliptic curve cryptography. In this scheme any node can transmit n number of message without threshold problem. This service is usually provided through the deployment of a secure message authentication code (MAC)**.**

VII. ACKNOWLEDGMENT

This research was supported in part by NSF grants CNS-0845812, CNS-1117831, CNS-1217206, and ECCS-1232109.

REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in IEEE INFOCOM, March 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," in IEEE Symposium on 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," in 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," in IEEE INFOCOM, April 2008.
[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," in IEEE Symposium on Security and Privacy, May 2000.
[6] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," in Advances in Cryptology (EUROCRYPT),pp. 387–398, 1996.
[7] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84–88, February 1981.
[8]T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Schemes on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

BIOGRAPHY

V.GAYATRI is Associate Professor, Dept. of CSE, GEETHANJALI INSTITUTE OF SCIENCE & TECHNOLOGY –NELLORE, AP, INDIA.Her research interested inHigh Privacy through Hop-by-Hop Message Authentication in Wireless Sensor Networks.

CH.VENKATESWARLU is M.Tech Student, Dept. of CSE, GEETHANJALI INSTITUTE OF SCIENCE & TECHNOLOGY – NELLORE, AP, INDIA.His research interested inHigh Privacy through Hop-by-Hop Message Authentication in Wireless Sensor Networks.

T.VENKATAPATHI is M.Tech Student, Dept. of CSE, GEETHANJALI INSTITUTE OF SCIENCE & TECHNOLOGY – NELLORE, AP, INDIA. His research interested inHigh Privacy through Hop-by-Hop Message Authentication in Wireless Sensor Networks.