ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Scalable Message Authentication System Based on Elliptic Curve Cryptography in Wireless Sensor Networks

Priyanka Boddu
M.Tech (CSE),
Department of CSE,
Gonna Institute of Engineering and Technology,
Andhra Pradesh, India.

Mr.Rambabu
Assisatnt Professor,
Department of CSE,
Gonna Institute of Engineering and Technology,
Andhra Pradesh, India.

Abstract:

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness 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 propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering 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 more efficient than the polynomial-based approach in terms of computational and communication overhead under comparable security levels while providing message source privacy.

Introduction:

1. Towards Resilient Geographic Routing in WSNs In this paper, we consider the security of geographical forwarding (GF) – a class of algorithms widely used in ad hoc and sensor networks. In GF, neighbors exchange their location information, and node forwards packets to the destination by picking a neighbor that moves the packet closer to the destination. There are a number of attacks that are possible on geographic forwarding.

One of the attacks is predicated on misbehaving nodes falsifying their location in- Formation. The first contribution of the paper is to propose a location verification algorithm that addresses this problem. The second contribution of the paper is to propose approaches for route authentication and trust-based route selection to defeat attacks on the network. We discuss the Proposed approaches in detail, outlining possible attacks and defenses against them.

2.On Optimal Information Capture by Energy-Constrained Mobile Sensors:

A mobile sensor is used to cover a number of points of interest (PoIs) where dynamic events appear and disappear according to given random processes. The sensor, of sensing range r, visits the PoIs in a cyclic schedule and gains information about any event that falls within its range. We consider the temporal dimension of the sensing as given by a utility function which specifies how much information is gained about an event as a function of the cumulative sensing or observation time.

It has been shown in [1] that for Step and Exponential utility functions, the quality of monitoring (QoM), i.e., the fraction of information captured about all events, increases as the speed of the sensor increases. This work, however, does not consider the energy of motion, which is an important constraint for mobile sensor coverage. In this paper, we analyze the expected information captured per unit of energy consumption (IPE) as a function of the event type, the event dynamics, and the speed of the mobile sensor.

Our analysis uses a realistic energy model of motion, and it allows the sensor speed to be optimized for information capture.We present extensively simulation results to verify and illustrate the analytical results.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3. Security Solutions for Wireless Sensor Networks:

This paper describes security solutions for collecting and processing data in Wireless Sensor Networks (WSNs). Adequate security capabilities for medium and large scale WSNs are a hard but necessary goal to achieve to prepare these networks for the market. The paper includes an overview on security and reliability challenges for WSNs. and introduces a toolbox concept to support such a framework.

Existing system:

In existing system, we propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, our scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. We develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity through hop by hop message authentication process. In order to evaluate the existing message authentication, SAMAC act as resilience to active and passive attack. In the existing system, 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 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 the existing system. 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 the existing system 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.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 elliptic curve cryptography (ECC) shows 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.

The existing anonymous 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 mix servers (with at least one being trusted). In a mix net, 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 mix net-like protocols rely on the statistical properties of the background traffic, they cannot provide provable anonymity. DC-net 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.

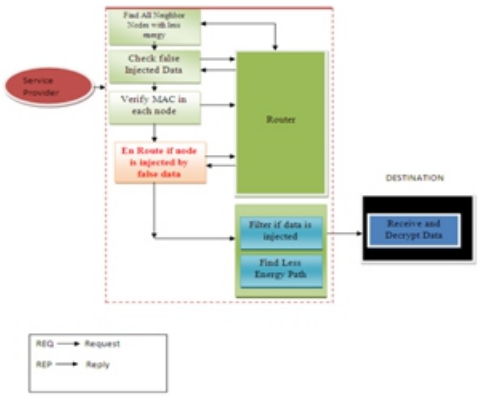
Proposed system:

The proposed system concentrates on providing high privacy to the message authentication. In addition to hop by hop message authentication, key exchange mechanism is enhanced through diffie Hellman key exchange algorithm. The source node encrypts the data using the public key of receiver node, and then transmits the data. After receiver receiving the data, it needs a private key for decrypting data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 the malicious node to get a key from key server.

System Architecture:



Modules description
Node Deployment

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

SAMA 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.

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. This can be done through the verification of public key. ACK is replied to previous hop node if authentication is successful.

COMPROMISED NODE DETECTION PROCESS:

If a message is received by the sink node, the message source is hidden in an AS.

Since the SAMA scheme guarantees that the message integrity is unhampered, when a bad or meaningless 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 difficult for the node to be identified without additional network traffic information. However, when a compromised node transmits more than one message, the sink node can narrow the possible compromised nodes down to a very small set.

Key server management:

Key server is a certificate authority server, which is responsible for message authentication. The key server verifies the information and authenticates the user. This could be a kind of data encryption and decryption process. This is achieved through diffie hellman key exchange algorithm.

Algorithm:

for each location l do /* initialize the belief */

$$Bel(L_0 = l) \leftarrow P(L_0 = l) \quad (17)$$

end for

forever do

if new sensory input s_T is received do

$\alpha_T \leftarrow 0$

for each location l do /* apply the perception model */

$$\widehat{Bel}(L_T = l) \leftarrow P(s_T \mid l) \cdot Bel(L_{T-1} = l) \quad (18)$$

$$\alpha_T \leftarrow \alpha_T + \widehat{Bel}(L_T = l) \quad (19)$$

end for

for each location l do /* normalize the belief */

$$Bel(L_T = l) \leftarrow \alpha_T^{-1} \cdot \widehat{Bel}(L_T = l) \quad (20)$$

end for

end if

if an odometry reading a_T is received do

for each location l do /* apply the motion model */

$$Bel(L_T = l) \leftarrow \int P(l \mid l', a_T) \cdot Bel(L_{T-1} = l')\, dl' \quad (21)$$

end for

end if

end forever

Tab. 1. The Markov localization algorithm

Steps for Sha1 Algorithm

SHA1 can be accessed through a Generic class called Message Digest.

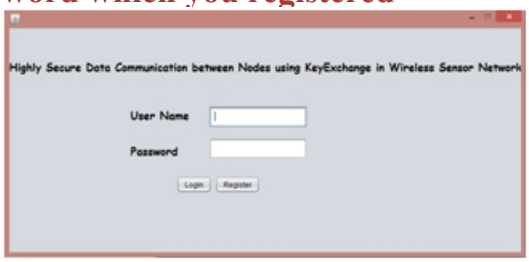
1). Generate a Message Digest object using get instance method of Sha1.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

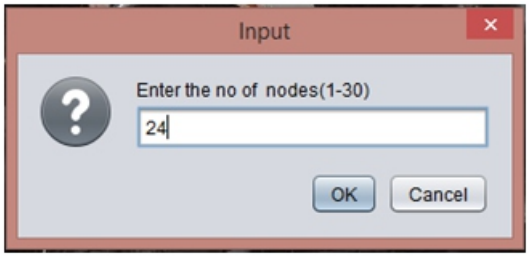
2).Call the Digest () Method: Performs SHA1 algorithm on the current input message and returns the message digest as a byte array.
3). Give the Input as a File which u want's a mac to be generated.
4).Read the Output to the Big integer variable which is used to translate a byte array containing the two's-complement binary representation of a BigInteger into a BigInteger.

Screen Shots:

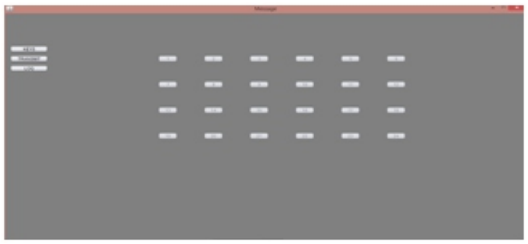
Step1: login to the system using username and password which you registered



Step2: Enter number of nodes

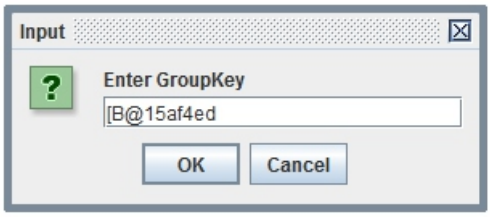


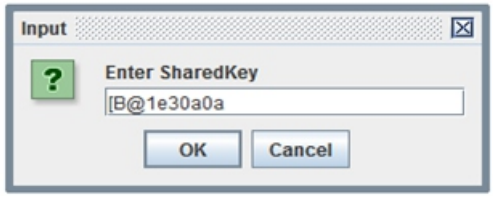
Step3: You get the display page with nodes



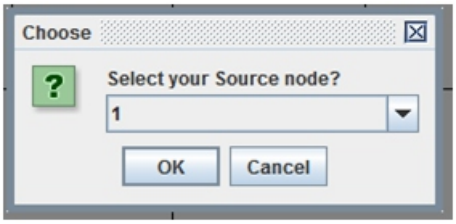
Step4: click the key button to get the grouped key and secret key

Step5: Then click the Transit button and you get two key pages which are grouped and secret keys.

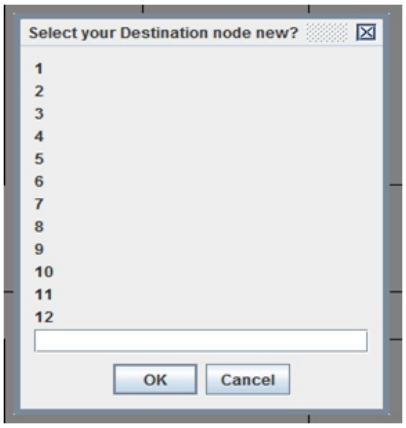




Step6: Now select the source node

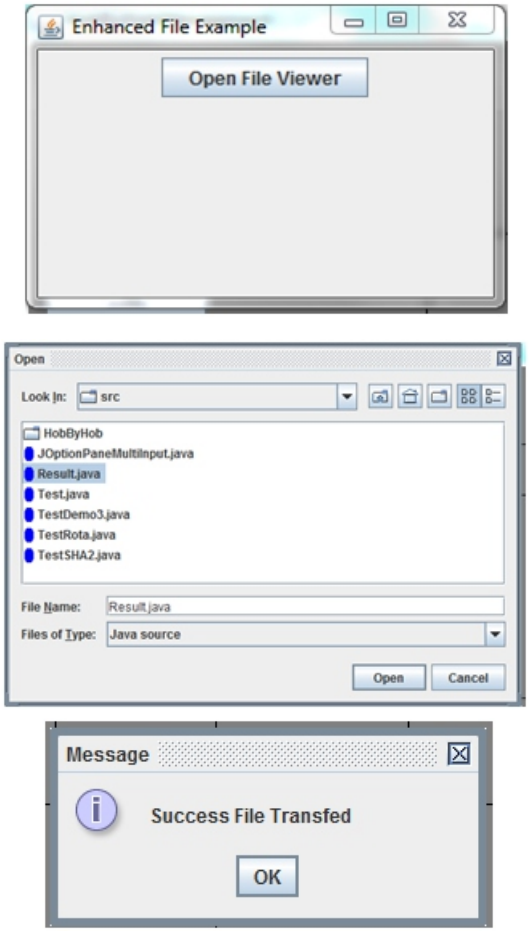


Step7: Select the destination node



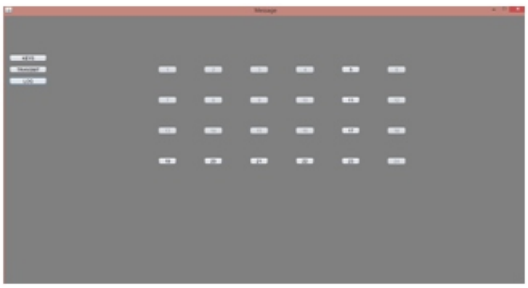
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Step8: Select your required file to send



File sent in encrypted form.

Step8: Display of the path of file sent



CONCLUSION:

In this paper, we first proposed a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity.

To provide hop-by-hop message authentication without the weakness of the builtin threshold of the polynomial-based scheme, we then propose a hop-by-hop message authentication scheme based on the SAMA. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification. We compared our proposed scheme with the bivariate polynomial-based scheme through simulations using ns-2 and TelosB. Both theoretical and simulation results show that, in comparable scenarios, our proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

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, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromiseresilient message authentication in sensor networks," in IEEE INFOCOM, Phoenix, AZ., April 15-17 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] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking crypto-graphic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1978.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[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," in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[11] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84–88, February 1981.

[12] ——, "The dinning cryptographer problem: Unconditional sender and recipient untraceability," Journal of Cryptology, vol. 1, no. 1, pp. 65–75, 1988.

[13] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, unobservability, pseudonymity, and identity management a proposal for terminology," http://dud.inf.tu-dresden.de/literatur/Anon Terminology v0.31.pdf, Feb. 15 2008.

[14] A. Pfitzmann and M. Waidner, "Networks without user observability– design options." in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 219, 1985, pp. 245–253.

[15] M. Reiter and A. Rubin, "Crowds: anonymity for web transaction," ACM Transactions on Information and System Security, vol. 1, no. 1, pp. 66–92, 1998.

[16] M. Waidner, "Unconditional sender and recipient untraceability in spite of active attacks," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 434, 1989, pp. 302–319.

[17] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," Journal of Cryptology, vol. 13, no. 3, pp. 361– 396, 2000.

[18] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discret logarithm," Electronics Letters, vol. 30, no. 24, pp. 2025–2026, 1994.

[19] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 950, 1995, pp. 182–193.

[20] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Advances in Cryptology–ASIACRYPT, ser. Lecture Notes in Computer Science, vol 2248/2001. Springer Berlin / Heidelberg, 2001.

[21] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in CCS'93, 1993, pp. 62–73.

[22] BlueKrypt, "Cryptographic key length recommendation," http://www. keylength.com/en/3/