International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Message Authentication and Source Privacy in Wireless Networks

Vaishali Kisanrao Gulhane[1], S. N. Shelke[2]

[1]Savitribai Phule Pune University, Sinhgad Academy of Engineering, Pune, India

[2]Professor, Savitribai Phule Pune University, Sinhgad Academy of Engineering, Pune, India

Abstract: ***Message authentication is a standout amongst the best approaches to ruin unapproved and defiled messages from being sent in wireless networks. Hence, numerous message validation plans have been produced, in view of either a symmetric-key cryptosystem or an open key cryptosystem. The vast majority of them, then again, have the impediments of high computational and correspondence overhead notwithstanding absence of adaptability and versatility to hub trading off assaults. To address these issues, a polynomial-based plan was as of late presented. On the other hand, this plan and its augmentations all have the shortcoming of an implicit edge controlled by the level of the polynomial: when the quantity of messages transmitted is bigger than this edge, the enemy can completely recuperate the polynomial. we propose an adaptable confirmation plan taking into account elliptic curve. While empowering middle of the road hubs validation, our proposed plan permits any hubs to transmit a boundless number of messages without anguish the limit issue. In addition, our plan can likewise give message source protection using Block Authentication Code(BAC). The proposed system plan more proficient than the polynomial-based methodology regarding computational and correspondence overhead under similar security levels while giving message source protection.***

Keywords: Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless networks, distributed algorithm, decentralized control, Block Authentication Code (BAC)

1. Introduction

Wireless sensor systems disentangle the collection and analysis of information from various areas. Target following and perimeter interruption identification applications advantage from the specially appointed arrangement and self-association capacities of wireless sensor systems. In any case, sensor systems conveyed in threatening situations must be strengthened against assaults by adversaries. This thesis solves the security problem in wireless sensor networks deployed for surveillance and target tracking by applying appropriate security mechanisms to a target tracking method, Optimized Communication and Organization. Nodes of a wireless netowrk implement three main functionalities: sensing of the environment, aggregation and storage of recorded data and communication between the nodes. The communication between the nodes is particular important, because it is the only way for the sensing nodes to move recorded data to a node or machine which will store and Analyse it. WSN has been exceptionally prevalent and broadly utilized as a part of numerous Industries, Military area, Medical and street observation application, Food security, Manufacturing to sense parameters. A Future cutting edge society will see a developing dependence on and need for intense sensor systems with high adaptability, execution, and functionality with low power utilizations. There are bunches of points of interest of sensor system like simplicity of sending, amplified extent, adaptation to non-critical failure, mobility. Sensor and Actor system is gathering of modest sensors and performing artists and link between them. As sensor comprise of different registering subsystems like processor simple to computerized converter, handset and battery. Battery is the only wellspring of force for processing as they are conveyed in dangerous range. Each hub may be sensor or performing artist is battery driven, this limits the measure of energy accessible to hubs. In the event that battery is depleted, then hub falls flat. In the event that one hub fails in the system entire system may crumple because of the hub. Changing battery is exceptionally basic and troublesome procedure. Along these lines, to expand life of battery by reducing vitality utilization in framework may build the lifetime of hub. The radio subsystem is the real vitality shopper in WSN when contrasted with other subsystem. To control the force for transmission, controlling of radio mode is very much critical. The unmoving mode expends impressive measure of force, so it's ideal to switch off radio when hub is not in work. There is different algorithm and conventions have been created to minimize the vitality consumption. Wireless sensor networks simplify the collection and analysis of data from multiple locations. Target tracking and border interruption discovery applications advantage from the impromptu sending and self-association capacities of remote sensor systems. Be that as it may, sensor systems conveyed in threatening situations must be braced against assaults by foes. This proposal tackles the security issue in remote sensor systems sent for observation and target applying so as to follow fitting security instruments to an objective following strategy, Optimized Communication and Organization. Hubs of a WSN actualize three principle functionalities: detecting of nature, conglomeration and capacity of recorded information and correspondence between the hubs. The correspondence between the hubs is specific imperative, since it is the main route for the detecting hubs to move recorded information to a hub or machine which will store and dissect it. Security necessities to anticipate adjustment and insertion of false information into the system, which would some way or another change the general results. This can be accomplished utilizing Message Authentication Codes (MACs) which are appended to network bundles and accepted by the collector. Remote Sensor Network is a Single-reason outline implies serving

one particular application where as conventional system broadly useful configuration implies serving numerous applications. Vitality is the principle imperative in the outline of all hub and system parts in remote sensor system where as in customary system normal essential configuration concerns are system execution and latencies, vitality is not an essential concern.Sensor networks often operate in environments with harsh conditions where as in traditional network devices and networks operate in controlled and mild environments. In wireless sensor network physical access to sensor nodes is often difficult or even impossible where as in traditional network maintenance and repair are common and networks are typically easy to access.In wireless sensor network most decisions are made localized without the support of a central manager whereas Obtaining global network knowledge is typically feasible and centralized management is possible.Hop by Hop transport is a rule of controlling the stream of information in a system. With hop by hop transport, chunks of information are sent from node to node in a store-and-forward way. As hop by hop transport includes the source and destination node, as well as rather a few or the majority of the middle nodes too, it permits information to be sent regardless of the fact that the way in the middle of source and destination is not for all time associated amid correspondence.In any case, the End-to-end guideline claims that vehicle control ought to be implemented end-to-end unless executing hop by hop transport accomplishes impressively better execution. In addition,hop by hop transport requires per-stream state data at halfway hubs, which restrains its adaptability.Source Privacy: Identity and location privacy, Since the actual message source node will be hidden in the AS.A procedure to verify that messages come from the alleged source and have not been altered, Achieve message integrity,Increase efficiency, Achieve Message confidentiality. In data security, message auhtentication or information beginning validation is a property that a message has not been adjusted while in travel (data integrity) and that the getting party can check the wellspring of the message. Message authentication does not necessarily incorporate the property of non-repudiation. Message Authentication is ordinarily accomplished by utilizing message validation codes (MACs), verified encryption (AE) or digital signatures. A few cryptographers recognize "message authentication without mystery" frameworks - which permit the expected collector to confirm the wellspring of the message, however don't try hiding the plaintext substance of the message - from verified encryption systems. A couple of cryptographers have inquired about subliminal channel frameworks that send messages that seem to utilize a "message authentication without secrecy" framework, yet truth be told likewise transmit a secret message. Distributed Algorithm Runs on computer hardware constructed from interconnected processors, Used for Distributed computing, Sub-type of Parallel algorithm Executed concurrently, These Algorithm Make Scheme suitable for decentralized network.

2. Proposed System

In this system, the receiver should be able to verify whether a received message is sent by the node or not .Message integrity will be also verified like the receiver should be able to verify whether the message has been modified en-route by the adversaries. As previously Many message authentication schemes have been used to protect messages but these authentication schemes have the limitations of high overhead, lack of ability, node attacks and threshold problem. Message authentication has a main role in thwarting unauthorized and effected messages from being sent in networks to save the energy. limitations of high overhead, lack of ability, node attacks

Algorithm :

Key Generation : We consider the public parameters are: p, g, YA. They are defined as follows:

1) We take p a big prime number for which the discrete logarithm problem is difficult in Zp
2) We consider g 2 Z*p with order p-1 modulo p, being a prime factor for p-1
3) Sender has the pair of keys (XA, YA). XA is the private key and YA is the public key
4) XA2 Z * p with XA does not divide p-1
5) Senderˆ as public key is calculated function of Sender ˆ as private key, YA = gXAmodp

Signature Generation: We consider m to be the message signed by Sender

1) The signature of Sender of the message m is represented by the pair (r,s) where
2) r = gx mod p
3) s = m - XA * r/x mod (p-1)
4) and we define below the parameter x generated for each signature, x is chosen independently at random from Zp with x != (p-1) every time a message is to be signed by Sender

Signature Verification:

1) Given (m,r,s) we can verify wheather (r,s) is Senderˆ as signature on the message m by checking the following:
2) gm = * rs mod p
3) Reciever calculates the signature using his private key XB and the random parameter x, which has been generated only for signing the message m
4) The verification process is possible only using the public key of sender.

3. Module Description

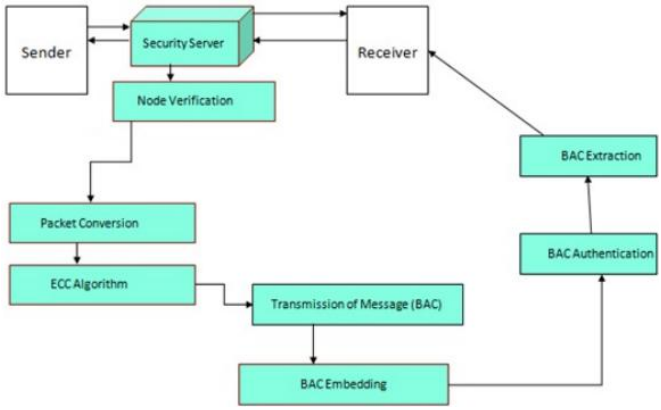

Figure 1: Architectural Diagram

Following phases/ Modules are there in the system

1) Loading phase,

2) Sensor Node Registration phase and
3) Message Generation phase.
4) Message verification Phase
5) Block Authentication Code

1) Loading Phase
Loading phase is actually a initialization phase where server detect automatically the number of the nodes available in the network. Create the data set for further operation like authentication and transfer of the message. Send a key to each for authentication purpose.

2) Sensor Node Registration Phase
Every sensor node has to register with the SS before starting communication with SS or other sensor node we can call it as a loading phase. Every sensor node can register to the security server with node name and its port number.
Security server will generate keys for respective nodes and maintains the log of node profile. In this phase node actually discover its id andits associated node.

3) Message generation Phase
Every node in the network will generate one message by using some code or byte of string and sending original message to the other node. These message will be transfer hop by hop to the destination node.

4) Message Verification Phase
When message get transfer successfully to the destination then authenticity is check and the decryption of the message will be happened. The server will also get notification for the successfully completion of the transfer.

5) Block authentication Code
In Data, the validation unit is an information block and the authentication code is produced taking into account the substance of the information block, in this way called Block Authentication Code (BAC). Information functions as follows: At the sender side, the verification data—BAC—is produced in view of a chose hash function with the bundle content and a generally concurred key as the information. In view of the estimation of every piece (0/1) of BAC, a few packets are planned to be conveyed with extra defers. At the collector side, the beneficiary extracts the embedded BAC taking into account the relative bundle postpone and contrasts the extracted BAC and the BAC generated taking into account the got content for validation. Scheme consists of BAC generation/BAC embedding and BAC extraction.

The proposed system is basically design to authenticate the message in network while transferring. The following are the key features of the proposed system.
1) Unconditional source anonymity can be provided by developing the original message authentication code using Elgamal on elliptic curve.
2) Efficient hop by hop message authentication can be achieved without the any limitation.
3) The scheme is prevented by node compromise attacks.
The nodes can be secure even if the other node gets compromised.
4) Efficient Key managements were introduced.
5) Confidentiality is maintained in proper way.

Here Security Server is responsible for all the security issue in the WSN. Server contains the all information of the chatting between the clients, the route, attacker ip in case of any attack etc. All notification regarding the operations are send to the server. While implementing such system we need Security server, Sensor node, Message etc. While implementation such system following Functional Requirements are consider .That are as follows:

Effective design of a message with public keys and Indexing of actual message sender, and maintaining anonymity with private keys.

The proposed system allows the user to deploy many Number of sensor nodes and hop by hop Authentication of sensor nodes by using Elliptical Curve Cryptography.

The system also considers both passive and active attacks and compromised nodes cannot create new public key.

The proposed system uses ElGamal signature scheme on elliptic curves for secure and efficient source authentication of nodes.

The proposed system also deploys the signature generation and verification on sensor nodes.

The proposed system efficiently gives the multi-hop Authentication for sensor nodes and the compromised nodes can be evaluated.

4. Results & Discussion

The system will be designed such that, it will overcome the limitation of overhead in computational and communication, scalability issue, Node Attack problems. It will also prevent unauthorized message and energy will be saved by reducing packet loss. The experimental results will show the effectiveness of message authentication & source privacy of different nodes.

5. Conclusion

The system will be Building trust relationships among Nodes can mitigate attacks of malicious messages.The main aim is to prevent unauthorized and corrupted messages being forwarded by allowing intermediate node authentication. We will be use our proposed module which will have both features i.e. message authentication and source privacy. Sender will able to hide their address by using source privacy schemeNodes will be able to prevent unauthorized message to transfer within the network. Proposed system will be able to overcome previous existing problems.

References

[1] A. Arul packiaraj1, M. Merlin Moses, ”Efficient Message Authentication and Source Privacy in Wireless Sensor Networks”, International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 1, pp: (222-227), Month: January - March 2015.
[2] C. Blundo, A. De Santis , A. Herzberg, S.Kutten, U. Vaccaro, and M. Yung, ”PerfectlySecure Key Distribution for Dynamic Conferences,” Proc. Advances in Cryptology (Crypto ˆ a92), pp. 471-486, Apr.1992.
[3] ”Cryptographic Key Length Recommendation,” http://www.keylength.com/en/3/, 2013.
[4] G.Dhivya, N.R.Jayashree ,”Message Authentication And Source Privacy Using BAC Technique In Wireless Sensor Networks ”,The International Journal Of Engineering and Science (IJES), Volume4, Issue 3 Pages ,PP.33-38,2015, ISSN (e): 2319 - 1813 ISSN (p): 2319 ˆ a 1805
[5] Guohua Ou1, Jie Huang, and Juan Li, (2010), ”A Key-Chain Based Key Management Scheme for Heterogeneous Sensor Network”, pp. 358-361.
[6] W.Zhang, N. Subramanian, and G. Wang, ”Lightweight and compromise resilient message authentication in sensor networks,” in IEEE INFOCOM, (Phoenix, AZ.), April 15-17 2008.
[7] ZohraBinteSailan, SyedaNusrath Fatima, M.Tech, ”Hop by Hop Message Authentication and Source Privacy in Wireless SensorNetworks”, International Journal MagzineofEngineerig, Technology, Managgement and Research,Vol.2: (2015, Issue No: 10 (October).
[8] H. Wang, S. Sheng, C. Tan, and Q. Li, ”Comparing SymmetricKey and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control,” Proc. IEEE 28th Int ˆ al Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.
[9] NithyaMenon, S.Praveena,” BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless Sensor Networks”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013,pp.112-115.
[10] Yun Li Jian Li JianRen, Jie Wu,” Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks”,the 31st annual IEEE Internat.
[11] A. Arul packiaraj1, M. Merlin Moses, ” Efficient Message Authentication and Source Privacy in Wireless Sensor Networks ”, International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 1, pp: (222-227), Month: January - March 2015.Journal MagzineofEngineerig, Technology, Managgement and Research,Vol.2: (2015, Issue No:10(October)
[12] G.Dhivya, N.R.Jayashree, ”Message Authentication And Source Privacy Using BAC Technique In Wireless Sensor Networks ”, The International Journal Of Engineering And Science (IJES) Volume 4 Issue 3 Pages PP.33-38 2015 ISSN (e): 2319 – 1813 ISSN (p): 2319-1805
[13] ”Cryptographic Key Length Recomendation ”, http://www.keylength.com/en/3/2013.
[14] A. Pfitzmann and M. Hansen, ” Anonymity, Unlinkability, Unobservability , Pseudonymity, and Identity Management a Proposal for Terminology, ” Feb. 2008
[15] D. Chaum, ”The Dinning Cryptographer Problem: UnconditionalSender and Recipient Untraceability,” J. Cryptology, vol. 1, no. 1,pp. 65-75, 1988.
[16] n Terminology v0.31.pdf, Feb. 2008.
[17] A. Pfitzmann and M. Waidner, ”Networks without User Observability Design Options.,” Proc. Advances in Cryptology (EUROCRYPT), vol. 219, pp. 245-253, 1985.
[18] M. Reiter and A. Rubin, ”Crowds: Anonymity for Web Transaction,”ACM Trans. Information and System Security, vol. 1, no. 1,pp. 66-92, 1998.
[19] M. Waidner, ”Unconditional Sender and Recipient Untraceability, in Spite of Active Attacks,” Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989.