ISSN No: 2348-4845

International Journal & Magazine of Engineering, Technology, Management and Research

A Peer Reviewed Open Access International Journal

Secure and Efficient Message Authentication Model for Source Privacy in Wireless Sensor Networks

Md Akram Uzaman
M.Tech Student,
Department of CSE,
B V Raju Institute of Technology,
Narsapur, India.

Ch.Kranthi Kumar
Assistant Professor,
Department of CSE,
B V Raju Institute of Technology,
Narsapur, India.

Abstract:

confidentiality and security to the data is actually provided by an authentication . Authentication involves the confident identification of one party by another party or a process of confirming an identity .But now a days there are various methods for authentication such as Message Authentication Code, Signcryption, Key Aggregate System are emerged very rapidly for better security precaution. This paper try to investigate how to provide authentication in wireless sensor networks. Other goals are to give an introduction to general security in wireless sensor networks. As Wireless sensor networks are the point of attention of numerous researchers regarding the security issue in the past several years. Message authentication is one of the most effective way to find out an intruder who can compromise with the nodes and can access to the data and corrupt the data in wireless sensor network. There were various methods have been developed to solve the problem such as symmetric key cryptography and public key cryptography. Each would have their own problems such as threshold overhead and key management and computation overhead and scalability .In order to solve such problem we developed a new authentication scheme using the elliptic curve cryptography .In this scheme any node can transmit n number of message without threshold problem. This paper is to do survey before actually implementing it.

Keyword:

Authentication, intruder, elliptic curve cryptography , symmetric key, public key.

I. INTRODUCTION:

The System which allows the sender to send a message to the receiver end in such a way that if the modified message will almost detected by Receiver that termed as message authentication.

We can also say that message authentication is data origin authenticity. Protecting the integrity of a message is done by message authentication. Each user while using message authentication expects that each and every message should be pass as in same condition that it was sent without adding any modified bits or extra characters. Wireless sensor have special characteristics because of total absence of infrastructure or administrative support these are wireless networks. They have limited bandwidth, energy constraints, low computational capabilities. Instead of all limitation WSN in useful in where is communication is done without infrastructure support. Security is the major constraint in WSN ,as sensor node may be deployed by attacker and the privateinformation may get hacked . In many cases it is sufficientto secure data transfer between the sensor nodes and the base station. In particular, the base station must be able to ensure that the received message was sent by specific sensor node and not modified while transferring. Many WSN applications such as health-care monitoring systems or military domains needs strong and lightweight authentication schemes to secure data from unprivileged users. That is really insecure. To over come all such security issue many different scheme that had been discover. Some schemes deals with detecting the compromised node , or detecting the injected false message in the network or giving special authorization to the sender or receiver, Encryption of decryption is the famous method for providing the security. WSN have various security challenges due to its nature these challenges are like Communication, resource , sensor node limitation, lack of fixed infrastructure ,unknown network ,topology for deployment. In wireless sensor network the unofficial and corrupted massage can be effectively prevented by message authentication. We can say message authentication is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. accidental and intentional message changes, offers a integrity of message while the message's origin affirms authenticity .

Until now various authentication schemes have been proposed to provide message authenticity and integrity verification for wireless sensor networks (WSNs). symmetric-key cryptosystems or public-key cryptosystems are the schemes Most of them, have various limitations like high computational and communication overhead , lack of scalability , node compromise attacks. I have mention some schemes that actually implemented for preserving the security of WSN through authentication method.

II. LITERATURE SURVEY:

Efficient Authentication over lossychannel[1] paper introduced efficient schemes, TESLA and EMSS, for secure lossy multicast streams. TESLA, short for Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, strong loss robustness, high scalability, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, short for Efficient Multi-chained Stream Signature, provides no repudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification. Attacking cryptographic scheme[2] show attacks on several cryptographic that have recently been proposed for achieving various security goals in sensor networks. They also told that these schemes all use “perturbation polynomials” to add “noise” to polynomial- based systems that offer information theoretic security, in an attempt to increase the resilience threshold while maintaining efficiency. They show that the heuristic security arguments given for these modified schemes do not hold, and that they can be completely broken once we allow even a slight extension of the parameters beyond those achieved by the underlying information-theoretic schemes R.L. Rivest, A. Shamir, and L. Adleman[3] proposed a Method for Obtaining Digital Signatures and Public-Key Cryptosystems. They also show that a message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar. The security of the system rests in part on the difficulty of factoring the published divisor, n Comparing Symmetric-Key and Public-Key Based Security Schemes[4] proposed a system that builds the user accesscontrol on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience. They also does work to provides insights in integrating and designing public-key based security protocols for sensor networks. The signature scheme introduced by author David Pointcheval and Jacques Stern[5] .In this paper, they address the question of providing security proofs for signature schemes in the so-called random oracle model . They establish the generality of this technique against adaptively chosen message attacks. Our main application achieves such a security proof for a slight variant of the El Gamal signature scheme where committed values are hashed together with the message.Ashwini M. Rathod and Archana C. introduces A Secure Network Discovery by Message Authentication[6] in Wireless Sensor Network in this paper, they propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate node authentication, that scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. Their system also proposed source privacyDining cryptographer scheme[7] works on preserving security for message authentication over the destination Keeping data confidential that who sends message to whom in a world where any transmission can be traced to its origin. This problem solved by author is unconditionally or cryptographically secure based on one time used key or public keys .Here author actually encrypt the message with intended recipient public keys to ensure the secrecy. The sender keeps the identity of the recipient secret. Also arrange the prefix to each message that the recipient only need decrypt the message with recognized prefixed .A Different prefix in used each time. New prefix could be agreed in advance, generated cryptographically as needed. Author shows that a public key distribute system can be used to construct a computationally secure sender untraceably channel .

a Statistical En-route Filtering (SEF)[8] mechanism that can detect and drop such false reports. We all know that a sensor network composed of a large number of small sensors. These sensors nodes area not equipped with temper resist sent network. Here the major issue of security compromises in large scale sensor network. In Large scale sensor network detecting and purging bogus reports injected by compromised node is a greater challenge .When a node in compromised all into store in that node become accessible. These node successfully provide bogus reports to its neighbours which results in manipulated solution. Such problems can be solved by asymmetric cryptography is in feasible so author provides new technique of statistical enroute filtering were SEF exploits dense deployment of sensor network.

For preventing a node to break down SEF carefully limits amount of information assigned to any node, and releases on the collective decision of multiple sensor for false report. When any sensoring report is forwarded to any node each sending node verifies the correctness of the MAC.s carried with certain probability the report is dropped on in correct MAC. Here purpose a key assignment method is designed for enroute detection of false report. They devise a mechanism for collective data report generation, enroll report, filtering and sink verification .Her the author proves that SHE is efficient at detecting dropping such false report injected by compromised node. It can filter out the 80% to 90 % false data by a compromised node.ElGamal [9] Public key cryptography is applied for digitalsignature. Elgamal also have security on the discrete logarithm problem .Here improved Elgamal algorithmmakes more extensive application in the field of authentication and e commerce . Here author included a new improved Elgamalalgo over a old Elgamal algorithm which is more efficient .They also tried to show the difference between them mainly in adding the random number to make original more complicated and more difficult to decipher .In case if Elgamal the hackers apparently need to solve logarithm for three times then test solution and test each solution need to go through an inverse element and exponential.

This makes the new Elgamal more complex .Here the authors work concentrate their work on enhancing security of random number. Also provide more complex link between the random number and private key .So that hackers can not use random number to attack the private key indirectly. an interleaved hop-by-hop authentication scheme[10] is implemented for perfect authentication .In militating application we always need to monitor the opponents activity .Theses can be achieve by clustering g certain group of nodes forinterested area and we can also create a base station in a secure location to control the sensor and to collect the data.A hacker the main culprit may compromised sensor node then use the same node to inject the false or wrong data to network. Here author focus his work towards the false injection attacks. As per his scheme base station is responsible for enabling the authenticity of report. scheme filter out the false injected packet into the network by compromised node before reaching towards the base station. Author make the use of various node like line node initialization, deployments phase, association discovery nodes to discover ids of the associated node, Report endorsement to generate the report, Enroute filtering to filter out the impacted node ,base station verification after receiving. Authors main intention to provide the security while transmission of packets. a ring signature[11], which makes it possible to specify a set of possible signers without revealing which member actually produced the signature. Unlike group signatures, ring signatures have no group managers, no setup procedures, no revocation procedures, and no coordination. The actual contribution is a new construction of such signatures which is unconditionally signer-ambiguous, provably secure in the random oracle model, and exceptionally efficient: adding each ring member increases the cost of signing or verifying by a single modular multiplication and a single symmetric encryption.

Network without user observatory [12] deals with keeping relationship between the sender and receiver unobservable for security purpose. Author introduced various Anonymity concept related to Receipt and sender anonymity. Recipient anonymity deals with Implicit address inoder to address the correct recipient. The unlink ability of sender and recipient is realized by special special network station called MIX. The main aim if MIX is to collect the number of message from the sender and changes their encoding and forward the message to recipient in different order. This way the author controls to hide the relationship between the sender and recipient .But the MIX controlled sender anonymity by generating at lease one keybit for each message bit and send each keybit to exactly one other user station over a secure channel. They also tried ti mention that many communication services where users now a days have to identify themselves can be used in an anonymous way in future.

Crowds[13] schemes Considering the users privacy author introduce a system crowds for protecting users anonymity on world wide web .Crowd is nothing but as a collection of users .Here in this paper crowd represented by a process on on computer called Jondo. When Jondo started its contacts a server called a blender to request admittance to the crowd. If admitted the blender report to the jondo the current membership information of the crowd and information that enables this jondo to participate in the crowd. Here jando picks a jondo from the crowd at random and forward the request to it. This approach works by grouping web users into a geographically diverse collection called a crowd. Here crowds retrieve the information on it's user behalf by way of a simple randomized routing protocol. This paper actually good example that shows that everyman should know that his conversation ,his correspondence and his personal life are private. The lack of transactions on WWW can be recovered by any way.Perfectly secure key distribution schemes[14] for dynamic conferences in this setting, an member of a group of t users can compute a common key using only his private initial piece of information and the identities of the other t&1 users in the group. Keys are secure against coalitions of up to k users; that is, even if k users pool together their pieces they cannot compute anything about a key of any conference comprised of t other users.

III. PROPOSED SYSTEM:

The proposed system is basically design to authenticate the message in network while transferring. There are variety if schemes were discus that follows the authentication method in order to provide the security. The following are the key features of the proposed system that give me the desire effect.

1)Unconditional source anonymity can be provided by developing the original message authentication code on elliptic curve.

2)Efficient hop by hop message authentication can be achieve 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.

IV. CONCLUSION:

In order to secure your communication message authentication in very important. Through proper message authentication only one can achieve great security. Security is the only seed that plant the proper tree of authenticity. This paper is a survey paper in order to investigate the different techniques available in message authentication. As per the further proceeding my plan is to develop the a 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).

REFERENCES:

[1]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.

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

[3]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.

[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. 11-18, 2008.

[5]D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361- 396, 2000.

[6]Ashwini M. Rathod, Archana C. S," Secure Network Discovery by Message Authentication in Wireless Sensor Network ",international Journal of Research in Engineering Technology and Management ISSN 2347 – 7539

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

[8]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.

[9]T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[10]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 .

[11]R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Advances in Cryptology (ASIACRYPT), 2001.

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

[13]M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transaction," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

[14]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.

[15]Waidner, "Unconditional Sender and Recipient Untraceability in Spite of Active Attacks," Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989.

[16]M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. ACM First Conf. Computer and Comm. Security (CCS '93), pp. 62-73, 1993.

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

[18]Jian Li, Yun Li, JianRen, Senior Member, IEEE, and Jie Wu, Fellow, IEEE,"Hop-by-Hop Message Authentication and Source Privacy in WirelessSensor Networks", ieee transactions on parallel and distributed systems, vol. 25, no. 5, may 2014