ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

Review on Design and Implementation of Hop to Hop Message Authentication and Source Privacy in Wireless Sensor Networks

Dipika R. Bisne[1], Mr. Punesh U. Tembhare[2]

P.G. Student, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, India [1]

Assistant Professor, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, India [2]

Abstract*:* In hop by hop message authentication with source privacy in wireless sensor network, were authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. Many message authentication schemes have been used to protect messages but these authentication schemes have the limitations of high overhead, lack of ability, to 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. Many authentication processes have been implemented to provide message authenticity and verification for wireless sensor networks. The symmetric-key based approach has complicated key management and lacks of ways. It is not taken to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The sender uses shared key to generate a message authentication code for each transmitted message. The authenticity and integrity of the message can verified only by the node using shared secret key, which is generally shared by a group of sensor nodes. An attacker can easily access the key by occupying a single sensor node. So, It will does not work in multicast networks.

In order to solve the problem, a secret based for the message authentication scheme was introduced. The method is similar to a threshold secret sharing, where it is determined by the degree of the value. This offers information security of the shared secret key when the number of messages transmitted is less than the threshold. The middle nodes verify the authenticity of the message. If the transmitted messages are larger than the threshold, can be fully recovered.

Keywords: Authentication schemes, multicast networks, key management, etc.

I. INTRODUCTION

In a design of hop by hop message authentication and source privacy in wireless sensor network. various mechanisms are used. In this mechanisms, hop to hop message authentication means that, messages would be transmitted from sender to destination through the various intermediate nodes. wireless communication guarantees that the sending message should be authenticated or not, in this mechanisms ,when message should be route, then this message may be corrupted. for this solution numbers of mechanisms are proposed. this message authentication mechanism can be implemented by wireless sensor networks. In security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks. A lot of authentication schemes had proposed in the past for protecting communication authenticity and integrity in wireless sensor networks. A novel message authentication approach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals.

II. MESSAGE AUTHENTICATIONS TECHNIQUES:

Statistical mechanism that can detect and drop such false reports. It requires that each sensing report be validated by multiple keyed message authentication codes, each message generated by a node that detects the same event. If the report is forwarded, all nodes along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. It exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes. Our analysis and simulations show that, with an overhead of 14 bytes per report, It is able to drop d false reports by a compromised node within limited forwarding hops, and reduce energy consumption in many cases. There is Public key cryptography scheme is used in existing system and proposed system is working on the three different techniques. these are, Public key cryptography based, Symmetric keys and hash functions and one way key chain based on hash functions.

In WSNs, it is usually assumed that public key cryptography can not be used because of the elaborate constraints. This means that the two communicating entities must use secret key functions and hash functions. In WSNs, there are two types of authentication: device level authentication and group level authentication. The device level authentication means that a message is proved to originate from a certain device, whereas the group level authentication means a message is proved to originate from a certain group of devices.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

Public key cryptography include those based on the RSA public key cryptosystem and Elliptic curve cryptography. TinyPK uses the lower exponent variant of the RSA public key cryptosystem to implement authentication of an external party.The external party is an entity that wishes to establish secure communication with the sensor network. The private part of the RSA is carried out at the certificate authority (CA). The nodes only need to implement the public parts.

In private keys and hash functions based schemes each symmetric authentication key is shared by a set of sensor nodes. If an intruder compromises a sensor node, the shared key will be disclosed. Hence these approaches are not resilient to a large number of node compromises. In one-way key chain type of schemes, the key hashed key chain and the techniques of delayed disclosure of keys are used. µTESLA and its variants are such approaches. In µTESLA, a key chain with delayed key disclosure is used to create an asymmetry in time among the broadcasting source (sinks or users) and the receiver (sensor node) to emulate public key cryptography. It having some limitations, these are communication overhead, memory overhead, computation overhead, less security.
These are various advantages of this technique, it reduces the storage overhead of the data. it reduces the probability for the guessing attack. it uses two way challenge and response authentication method, so it can prevent replay attacks.
In a BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless Sensor Networks model previously working on the existing system .there are some existing techniques which is***. Statistical En-route Filtering(SEF), Interleaved hop-by-hop authentication (IHA),Location-Based Resilient Secrecy (LBRS), Location-aware end-to-end data security design (LEDS), Bit-compressed authentication Technology***
And proposed system used ***BECAN scheme.***
This mechanism uses Message Authenticated Code (MAC).In detection of an event each report generated by the sensor nodes validated by multiple keyed message authenticated code (MACs). As the report being forwarded, each intermmidiate node along the way verifies the correctness of the MACs as early as possible. Sometimes the injected false data escapes the en-routing filtering and will be delivered to the sink. In that case it will verify the correctness of each MAC carried in each report and reject false ones. In this scheme the sensor node is associated with two other forwarding nodes along the path. The one closer to the base station is the upper associated node and the other is the lower associated node. An en-routing node will forward received report if it is correctly verified by its lower association node. This system adopts a location key binding mechanism. This will reduce the damage caused to node by an attacker and further reduces the false data generation in wireless sensor networks. This mechanism is provide end-to-end security efficient and high data availability. LEDS uses a symmetric key and location key management, to achieve high en-routing filtering. In this technology can achieve bandwidth-efficient by compressing MAC single bit. This provide high security.
Proposed system is to achieve bandwidth-efficient authentication for filtering injected false data. Every sensor node in wireless sensor network shares a private key with the sink. Each node knows its one-hop neighbours and establish a public-private key pair with each of them. In this scheme it use Message Authentication Code (MAC) mechanism to authenticate broadcast messages and every node can verify the broadcast messages. there is some limitations of these scheme:Energy wasted in en-route nodes of wireless sensor network. There is a heavy verification burden at sink. There is no cooperative authentication among en-routing nodes.
This scheme having some advantages: Save energy by early detecting and filtering the majority of injected false data. It achieves not only high filtering probability but also high reliability. It also adopts the bit-compressed authentication technique to save the bandwidth.
In A Survey Paper on Hop by Hop Message Authentication in Wireless Sensor Network paper introduced efficient schemes TESLA and EMSS, Attacking cryptographic scheme, Symmetric-Key and Public-Key Based Security, Elliptic curve cryptography (ECC),Dining cryptographer, Statistical En-route Filtering (SEF), ElGamal Public key cryptography and Crowds. The proposed system is basically design to authenticate the message in network while transferring. The scheme is Hop by Hop message Authentication.
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.
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 toincrease the resilience threshold while maintaining efficiency.
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 ElGamal signature scheme where committed values are hashed together with the message.

DOI 10.17148/IJARCCE.2015.4136

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

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 privacy.

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 Statistical En-route Filtering (SEF) 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.

ElGamal Public key cryptography is applied for digital signature. Elgamal also have security on the discrete logarithm problem .Here improved Elgamal algorithm makes more extensive application in the field of authentication and e commerce . a new improved Elgamal algo over a old Elgamal algorithm which is more efficient .The difference between them mainly in adding the random number to make original more complicated and more difficult to decipher.

Crowds schemes Considering the users privacy author introduce a system crowds for protecting users anonymity on world wide web .Crowd is a collection of users .Here 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.

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

Efficient hop by hop message authentication can be achieve without the any limitation.

The scheme is prevented by node compromise attacks. The nodes can be secure even if the other node gets compromised.

Efficient Key managements were introduced.

There was some limitations;

Threshold overhead for message transmition.

Key management and computation overhead

Less scalability of the network.

These also includes more advantages;

A new efficient authentication scheme using the elliptic curve cryptography.

This service is usually provided through the deployment of a secure message authentication Code (MAC)**.**

Secure Network Discovery by Message Authentication in Wireless Sensor Network paper introduced efficient schemes; Symmetric Key and Hash Based Authentication, A Secret Polynomial Based Message Authentication Scheme, perturbation polynomials Cryptology, Public Key Based Approach.

And proposed model worked on; Source anonymous message authentication code (SAMAC), Message authentication code (MAC), Hop by hop message authentication, Compromised node detection, Source privacy, and Key server management.

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.

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 thresh-old, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation.

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, to thwart the adversary from computing the coefficient of the polynomial.

For the public-key based approach, each message is transmit-ted 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. there are some limitations;

It requires initial time synchronization, which is not easy to be implemented in large scale WSNs. It also introduces delay in message authentication, and the delay increases as the network scales up.

Its advantages are the follows;

Any node to transmit an unlimited number of messages without suffering the threshold problem. It also provide message source privacy.

Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks paper s includes the different techniques;

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

A polynomial-based scheme, public-key-based and symmetric-key-based approaches.

And proposed model operates on,Elliptic curve cryptography (ECC) and Hop-by-hop authentication.

A secret polynomial-based message authentication scheme was introduced in . This scheme offers information theoretic security with ideas similar to a threshold secret sharing scheme, 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.

An unconditionally secure and efficient source anonymous message authentication scheme (SAMA). Our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

These are the some limitations carried out by existing system:

Computational overhead and Communication overhead and message transmission delay.

It also carried some advantages:

Allows any node to transmit an unlimited number of messages without suffering the threshold problem and This scheme can also provide message source privacy.

III. RESEARCH METHODOLOGY:

The proposed authentication scheme aims at achieving the following goals, Message authentication: The receiver should be able to verify whether a received message is sent by the node or not Message integrity: The receiver should be able to verify whether the message has been modified en-route by the adversaries. Hop-by-hop message authentication: Every forwarder on the routing path or network should be able to verify the authenticity and integrity of the messages upon each reception. Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or by the local traffic. Node compromise resilience: The scheme should be resilient to node compromise attacks. No matter how many nodes are compromised an d the remaining nodes can still be secure.

IV. COMPARATIVELY STUDY

Title	Techniques	Bandwidth	Pwer Consumption	Scalability	Reliabality
ADASHWSN	Public key cryptography based,symmetric key and hash functionOne waykey chain based on hash functions	Limited bandwidth	Pure power consumption	Less scalable	Less reliable
BECAN	becan	More bandwidth	Less power consumption	High scalable	High reliable
ASPHHMAWSN	Hop by Hop message Authentication	not specified	More consumption	More scalable	More reliable
SNDMAWSN	SAMA MAC Hop by hop message authentication. Compromised node detection Source privacy Key server management	Efficient bandwidth	Less power consumption	More scalable	More reliable
PHHASPWSN	ECC Hop-by-hop authentication	More efficient bandwidth	Moderate power consumption	More scalable	Less reliable

DOI 10.17148/IJARCCE.2015.4136

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

IV. CONCLUSION

The proposed authentication scheme aims at achieving the following goals, Message authentication: The receiver should be able to verify whether a received message is sent by the node or not Message integrity: The receiver should be able to verify whether the message has been modified en-route by the adversaries. Hop-by-hop message authentication: Every forwarder on the routing path or network should be able to verify the authenticity and integrity of the messages upon each reception. Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analysing the message contents or by the local traffic. Node compromise resilience: The scheme should be resilient to node compromise attacks. No matter how many nodes are compromised and the remaining nodes can still be secure.

REFERENCES

[1] Junqi Zhang1,2, Rajan Shankaran1, Mehmet A. Orgun1, Abdul Sattar2, and Vijay Varadharajan1," A Dynamic Authentication Scheme for Hierarchical Wireless Sensor Networks".

[2] Nithya Menon, 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.

[3] Prof N.R.Wankhade, Jadhav Ashvini B.," A Survey Paper on Hop by Hop MessageAuthentication in Wireless Sensor Network" , N.R.Wankhade et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8321-8324.

[4] Ashwini M. Rathod1, Archana C. S., "Secure Network Discovery by Message Authentication in Wireless Sensor Network", International Journal of Research in Engineering Technology and Management,pp.1-7.

[5] Yun Li Jian Li Jian Ren, Jie Wu," Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks",the 31st annual IEEE International Conference on Computer Communications,pp.3353-3357.

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

[7] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, 2009.

[8] 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.

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

[10] 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. 2008.

[11] 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.

[12] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering ofInjectedFalse Data in Sensor Networks," Proc. IEEE INFOCOM, Mar. 2004.

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

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

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

BIOGRAPHIES

Dipika R. Bisne received Graduate Degree in Computer Engineering in 2013 from RTMNU University, Nagpur. She is currently student of M.E. in wireless communication and computing branch, from RTMNU University, Nagpur.

Mr. P. U. Tembhare Received Graduate Degree in Information Technology from RTMNU University, Nagpur and M.TECH in Computer Science Engg. From RTMNU University, Nagpur. They are currently working as Asst. Prof. at P.C.E. Computer Technology Dept. PCE, Nagpur. Area of interest is Algorithm, Artificial Intelligence, Computer Network.