International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

DATA FLOW AUTHENTICATION AND PRIVACY IN WIRELESS SENSOR NETWORK

S. LEO ALBERT RAJASEKARAN[1], R. JAGAN[2], K. RAJAKUMARI[3]

[1,2]Final Year, B.Tech, Department of Computer Software Engineering
Bharath University, Tamilnadu, India.

[3]Assistant Professor,Department of Computer Science and Engineering
Bharath University,Tamilnadu, India.

Article Received: 20/03/2015 | Article Revised on:31/04/2015 | Article Accepted on:06/04/2015

ABSTRACT

Message Authentication is prevents unauthorized and corrupted messages from being forwarded in wireless sensor networks. This is implemented using scalable authentication scheme namely SAMA and MES. However message authentication has been developed based on symmetric key cryptosystems or public key cryptosystems. They have the limitations of high computation and communication overhead, lack of scalability and resilience and node compromise attacks. All the above mentioned drawbacks are overcome in the proposed system. Message authentication has a main role in thwarting unauthorized and effected messages from being sent in networks to save the energy. The method is similar to a threshold secret sharing, in this 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 exceeds the threshold then it can be fully recovered.

Keywords ; Multicast Networks ,Key Management, Authentication Schemes.

I.INTRODUCTION

A. Definition of wireless sensor network

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. In many WSN [7] applications, the sensor nodes are battery driven and they are often very difficult to recharge or change the batteries.

B. Sensor node

A sensor node normally consists of four basic components namely a sensing unit, a communication unit, a processing unit and a power unit. There are two kinds of sensor nodes used in the sensor network. In which the normal sensor node is deployed to sense the phenomena and the other is gateway node that interfaces sensor network to the external world.

C. Message Authentication

In hop by hop message authentication with source privacy in wireless sensor network, where authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. Many of the message authentication schemes have been

used to protect messages but these authentication schemes have the limitations of lack of ability, high overhead, to node attacks and threshold problem. Message authentication[6] 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.

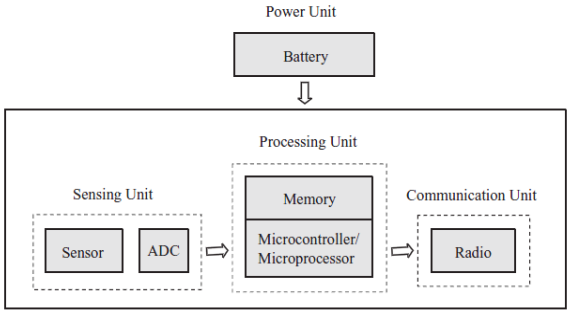

Figure 1: Sensor node

Analytical mechanism that can detect and drop such false reports. Multiple keyed message authentication codes is used in each sensing report to validate each message which has been 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 earlier points. Remaining false reports is filtered out by sink that escape the en-route filtering which 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. This analysis and simulations show that, with an overhead of fourteen 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 cannot 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.

Public key cryptography includes 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 node. If an intruder by_passes 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 Enroute 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 intermediate 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 neighbors and establish a public-private key pair with each of them. In which 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[5], short Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, minimal overhead, high scalability, strong loss robustness, and, at the cost of loose initial time synchronization and slightly delayed authentication. Efficient Multi-chained Stream Signature (EMSS), provides no repudiation of origin, low overhead, and high loss resistance 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 security theroitally, in an attempt to increase the resilience threshold while maintaining efficiency.

I.Related Works

In papers [5], [6], symmetric key and hash based authentication techniques were projected for WSNs. In these techniques, each symmetric authentication key is shared by a cluster of sensor nodes. An intruder is possible to compromise the key by capturing the single sensor node. Therefore, these techniques are not flexible to node compromise attacks. A secret polynomial based message authentication technique was discussed in [7]. This scheme presents information-theoretic security with ideas akin to to a threshold secret, in which the threshold is determined by the degree of the polynomial. If the number of message transmitted is less the threshold, the technique facilitates the intermediate node to confirm the authenticity of the message through polynomial evaluation. But, when the count of messages transmitted is greater than the threshold, the polynomial can be fully improved and the system is completely broken. To boost the threshold and the complexity for the intruder to reconstruct the polynomial which are secret, random noise, which is also called as perturbation factor, was introduced to the polynomial in [8] to thwart the adversary from calculating the coefficient of the polynomial. Anyhow, the added perturbation factor can entirely removed using error-correcting code schemes [8]. For the public-key based

technique, each message is transmitted along with the digital signature of the message produced using the sender's private key. Sender's public key is used by every intermediate forwarder and the last receiver can authenticate the message. The recent development on elliptic curve cryptography (ECC) focuses that the public-key schemes can be more beneficial in terms of usage of memory , message complexity and security resilience. Hence public-key based techniques have a simple and clean key management [3].

I. **Wireless sensor networks (WSN)** have the lead over traditional networks in numerous ways such as large scale, autonomous nature and intense deployment [1],[4]. Likewise, it has improved fault tolerance because if a sensor node fails others can gather/proceed data. Because of its ad-hoc nature it grows to be more attractive in certain applications such as syndrome surveillance, military, environmental observation, fire detection, supply chain management, energy automation, vision enabling, gaming, building administration, health and other commercial and home applications [5]. With the extensive deployment of WSN for multi-faceted applications security is becoming a growing concern. For example, in a battleground, a military communication network used for susceptible information exchange can be hacked by its adversaries if the WSN has security holes causing stern loss of life and machinery. Security of WSN is a big challenge due to its limited resources such as power supplies, energy, computation, small memory and communication capabilities [9], [2], [4] Cryptographic algorithm performs a significant role in the security and resource conservation of wireless sensor networks (WSN) This paper spotlights a cryptographic and encryption scheme that produces Message Authentication Code (MAC) in wireless sensor networks (WSN), which is more practicable in the restricted resources of wireless sensor networks (WSN) and also supply good security in communication as well.

II. Existing System

Existing system is based on either symmetric key cryptosystems or public key cryptosystems. The symmetric key based approach requires complex key management. The shared key is used by the sender to generate a Message Authentication(MAC) for each transmitted Message. In this method the key is generally shared by a group of sensor nodes. The intruder able to compromise the key by capturing a single sensor node. To solve scalability Problem a secret polynomial based message authentication scheme was introduced which works based on threshold. Message authentication plays a key role in preventing unauthorized and corrupted messages from being forwarded in networks to save the sensor energy which is precious. Authentication of message schemes can be divided into two categories public key based approach and symmetric key based approaches.

The symmetric key based approach requires complex key management is not resilient to node compromise attacks since both sender and receiver have to share a same key. Compromise of key is done by by capturing a single sensor node an intruder.

The scalability problem is solved through, a secret polynomial based message authentication scheme was introduced. The idea is similar to a secret sharing threshold, where threshold is determined by the degree of polynomial and the intermediate nodes verify the authenticity of the message through a polynomial determination. If the number of messages transmitted is greater than the threshold value , adversaries are fully recovered and the system is completely broken. One of the limitations is the large computational overhead. The recent progress on ECC (elliptic curve cryptograph) shows that this can be more advantageous in resilience security and usage of memory.

An unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified Elgamal signature (MES) scheme on elliptic curves has been introduced. This Modified elgamal signature scheme is secure against adaptive chosen-message attacks in the random oracle model.

DISADVANTAGES OF EXISTING SYSTEM:

- High computational and communication overhead.
- Lack of scalability and resilience to node compromise attacks.
- Polynomial-based scheme have the weakness of a built-in threshold.

III. PROPOSED SYSTEM

A. **MES***(*Modified ElGamal signature)

The MES consists of 3 algorithms namely Key generation algorithm, Signature algorithm and verification algorithm

I.Key generation:

p->large prime number

g-> generator of Zp

for a random private key x which belongs Zp.

To public key y= gk mod p

IV.Sinature Algorithmm:

To sign a message 'm'

Choose random K which belongs to Zp-1

Copute r= gk mod p and solves s=rxh(m,r) + k mod(p-1)

Signature pair(r,s)

V.Verification algorithm:

Verifier checks whether signature equation

gs = ry mod p

then verifies accepts else rejects.

approach on a fixed set of attributes. To complement and strengthen social relationship, the second new layer is

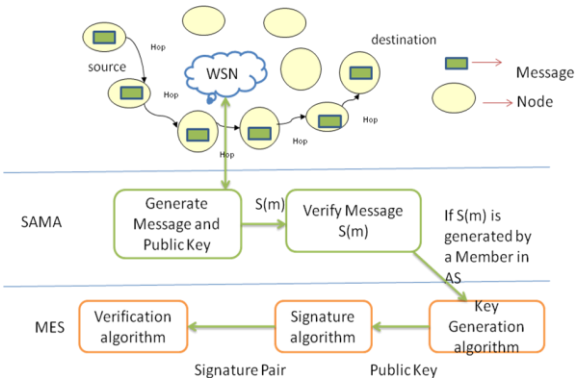

Figure:1 System Architecture

System Architecture consists of 3 partitions. First is the creation of nodes which issued by the wireless sensor networks. Let us consider a ambiguity set of nodes where the message is getting transferred from source to destination. Here the circles represents the nodes and the rectangles is the message.

While a node/sender wants to pass a message 'm' with public keys and encrypt the message using private key and the message as s(m).now the verifier in each intermediate node through which the message is getting transmitted verifies whether s(m)is generated by the member in the AS

When the verification gets over, if it is from the legitimate user in group message is passed else dropped.

VI.SYSTEM IMPLEMENTATION

A. *Modules*

When come to the module separation and implementation, this has been identified four distinct modules that together fulfill the entire functionality. And the main functionality that extends to the future expansion of the project. Mainly four important modules are identified namely

1) Node creation and message generation

- In this module The mobile nodes are designed and configured dynamically, designed to employ across the network, in which the nodes have the direct transmission range to all other nodes.
- A message 'm' is generated.

2) SAMA Message Authentication

- This module SAMA creates message 'm' With public keys namely K1,K2…Kn
- AS is Ambiguity set={a1,a2,…an}
- Where a is nodes in the set
- Sender is 'At' node where t=1 to n
- It creates a message S(m) using private key 'dt'

Algorithm: SAMA Message Authentication

Input : message 'm' with public key

Output : message S(m)

3) Hop-by-hop Message Authentication

- Every forwarder on the routing path should be able to verify the authenticity and the integrity of the message on reception. This can be done through the verification of public key.
- Verifier determines whether S(m) is generated by a member in the AS or not.

In MES Key generation algorithm ,signature algorithm and Verification algorithm is used for Message Authentication

Algorithm: Hop-by-hop Message Authentication

Input : message S(m)

Output : Authenticated message

4) *Compromised node detection Process*

- Since the SAMA scheme guarantees the message integrity , when a bad or meaningless message is received by the sink node, the source node is viewed as compromised.
- If the compromised node only transmits 1 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 1 message, the sink nodes can narrow the possible compromised nodes down to a very small set.

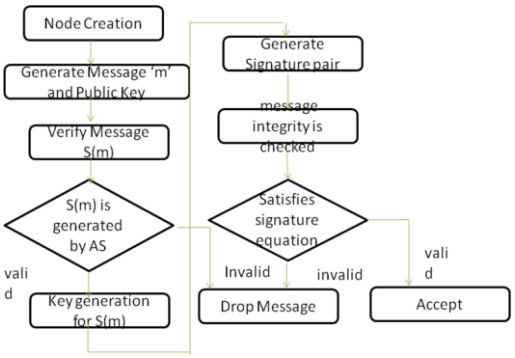

Figure:2 Flow chart Diagram

VII.RESULT AND ANALYSIS

A. Performance Analysis

Proposed system uses scalable authentication scheme based on elliptic curve cryptography. While enabling intermediate node authentication, In our proposed scheme which allows any node to transmit an unlimited number of messages without suffering the threshold problem.

B. Security Goals

Security assessments of any application spotlight on the five fundamental tenets of data security: non-repudiation, confidentiality, integrity of data, origin integrity, , and availability. The definitions used in this sub_section are derived from [36] and [37]. Confidentiality means the camouflage of information from unauthorized entities. Mechanisms used to accomplish confidentiality include access control mechanisms and cryptography.

C.Challenges

The lack of proficient authenticated messaging exposes all layers of the sensor network protocol stack to potential compromise. Without link-layer authentication, an attacker may insert unauthorized packets into the network. This may be used to introduce collisions and force legitimate nodes into an infinite waiting state

D. Attacks against Sensor Networks

Physical tampering poses a threat to sensors. If sensors are distributed in an unprotected area, an attacker could destroy the nodes or collect the sensors, analyze the electronics, and steal cryptographic keys. This complicates the process of bootstrapping newly deployed sensors with cryptographic key material. To protect against this, sensors must be tamper-proof or they must erase all permanent and temporary storage when compromised.

CONCLUTION AND FUTURE WORK

A novel and efficient SAMA based on ECC is proposed which can provide source anonymity. Efficient Hop-by-hop message authentication mechanism is done.Source node privacy protection is devised with isolation of the compromised nodes.

REFERENCES

[1]. 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.

[2] 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.

[3] 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.

[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008. TABLE 3 Memory (KB) for the Two Schemes (TelosB) (F Stands for Flash Memory).

[5]. A. 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.

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

[7] 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.

[8] 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.

[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," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[10] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387- 398, 1996.