www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12049-12052

Towards Secure and Dependable Message Authentication in WSN

Kavitha M[1], Rekah H[2], Dr. Siddappa M[3]

[1] M. Tech, Department of CSE,
Sri Siddhartha Institute of Technology,
Tumkur Karnataka, India
neela.kavitha@yahoo.com

2 Assistant Professor, Department of CSE,
Sri Siddhartha Institute of Technology,
Tumkur, Karnataka, India

3 Head of the Department, Department of CSE,
Sri Siddhartha Institute of Technology,
Tumkur, Karnataka, India

Abstract: ***In recent years, Wireless Sensor Network (WSN) finds applicability in every domain namely the military, health care, structure monitoring, forest surveillance, agriculture, etc, as they can be deployed in unattended hostile environment. WSN will be an integral part of human lives. However one of the main concerns in WSN is its limited resources. Wireless sensor networks consist of one or more base stations and a number of sensor nodes that get stimulated from external events. This paper provides message authentication scheme in wireless sensor networks. Message authentication is the effective ways to prohibited unauthorized users and unwanted messages forwarded in wireless sensor networks. Many message authentication methods have been developed, based on either public-key or symmetric key cryptosystems. But most of them have the lack of scalability, limitations of high computational and communication overhead, resilience to node compromise attacks and threshold problem. To solve such problem, a new authentication scheme has been developed using the elliptic curve cryptography. This scheme proposes any node can transmit any number of messages without threshold problem and also provide message source privacy.***

Keywords: symmetric-key cryptosystem, public-key cryptosystem, source privacy, wireless sensor networks (WSNs).

1. Introduction

A Wireless Sensor Networks (Figure 1) consists of a large number of resource constrained sensor nodes that are spatially distributed in a hostile environment and with the resource rich node called as the Base Station (BS). The sensor nodes task is to sense physical phenomena from its immediate surroundings, process and transmit the sensed data to the other nodes or Base stations.

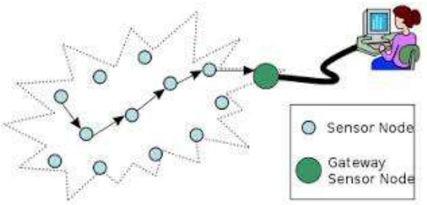

Figure 1: Wireless Sensor Network

The development of wireless sensor networks was motivated by military applications. Today such networks are used in many consumer and industrial applications, such as health-care monitors systems, tracking and controlling systems, industrial process monitoring and control, and so on.

Wireless sensor networks introduce far more challenges than wired networks towards design of efficient security solution. Communication media is the air where everybody has access. It can perform variety of active and passive attacks on traffic due to broadcast nature of the communication. Energy is the biggest concern because sensor nodes operate on battery and it may not be possible to visit large number of nodes to replace their batteries. The biggest energy consuming operation for a sensor node is the communication. Thus, security solutions with large communication overhead are not feasible.

In cryptography, a message authentication code (MAC) is a piece of information used to authenticate a message and to provide authenticity and integrity assurance on the message. Authenticity assurances affirm the message origin and Integrity assurance detects intentional and accidental message changes.

Message authentication plays a key role in removing corrupted and unauthorized messages being forwarded in networks to save the valuable sensor energy. For this reason, many authentication methods have been proposed in literature to provide message integrity and authenticity verification for wireless sensor networks.

2. Threat Model And Assumptions

We assumed that, the wireless sensor networks are consist of a more number of sensor nodes and also we assume that in the sensor domain ,each sensor node knows its location and is able to communicating directly with its neighboring nodes .The entire network is fully connected through multi-hop communications. We assume there is a security server which is responsible for generation, distribution and storage of the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all type of information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can alter and controlled by the attackers. The compromised nodes however, will not be able to create new public keys. Based on these assumptions, this paper has two types of attacks introduced by the adversaries:

- Passive attacks: Through passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis.
- Active attacks: Once the sensor nodes are compromised, the adversaries will get all type of information stored in the compromised nodes. The adversaries can able to modify the contents of the messages, and inject their own messages.

3. Literature Overview

In Statistical En-route Filtering (SEF) mechanism [3] will detect and drop false reports. SEF needs each sensing report to be validated by number of keyed message authentication codes (MACs), each codes generated by a node that detects the same event. As the report is move forwarded, along the way each node checks the correctness of the MACs code and drops those with invalid MACs at earliest points. This scheme do not achieve resilient to node compromise attacks. SEF also does not address the issues of how to identify compromised nodes or revoke compromised keys. SEF is not designed to address all the attacks that a compromised node may launch, such as dropping legitimate reports passing through it, recording and replaying legitimate reports, or injecting false control packets to disrupt other protocols.

An interleaved hop-by-hop authentication scheme [2], guarantees the base station will detect any number of injected wrong data packets when it is not more than a particular number nodes are compromised. This scheme also gives an upper bound for the number of hops that before it is detect and dropped a false data packet may be forwarded, given that there are up to colluding compromised nodes. In this paper, present a simple authentication scheme is presented which prevent false data injection attacks in sensor networks. The scheme guarantees that the base station can detect a false report when no more than security threshold nodes are compromised.

A Message authentication approach which adopts an unsettled polynomial-based technique [3] to achieve the aim of immediate authentication, resilience to a large number of node compromises and scalability. Experiments and comprehensive analysis have being conducted to evaluate the scheme in terms of security. To increase the complexity and threshold of the intruder to reconstruct the secret polynomial, a random noise also known as perturbation factor, was added to the polynomial, to prevent the adversary from computing the coefficient of the polynomial. The added perturbation factor can be completely eliminated using error-correcting code techniques. A key distribution procedure for dynamic conferences is a method by which initially an (off-line) trusted server distributes private individual pieces of information to a set of users. Later any group of users of a given size is able to compute a common secure key.

A. Perrig, R. Canetti, J. Tygar, and D. Song, They research the applications and theory of perfectly secure systems [4], in this any group of n users can compute a common key. Each user computes by using his private piece of information and recognize of the other n - 1 user group. Keys are protect against association of up to k users, means even if some users join together their pieces it cannot compute anything about a key of any n-size conference comprised of other users. They consider a non-interactive model where without any interaction users compute the common key. They prove a lower limit on the size of the user's piece of information two times the size of the common key. Then they establish the most favorable of this limit, by explaining and understanding a scheme which exactly meets this limitation. They consider the model where interaction is allowed in the common key computation phase, and show a gap between the models by exhibiting an interactive scheme in which the user's information is only k + n - 1 times the size of the common key. After that they show useful and different modifications of the basic scheme.

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 many messages transmitted are below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when many messages transmitted are larger than the threshold, the polynomial can be fully recovered and the system is completely broken.

Efficient Authentication over lossy channel [5] proposes two schemes, TESLA and EMSS, for secure lossy multicast streams. TESLA (Timed Efficient Stream Loss-tolerant Authentication), offers sender authentication, EMSS (Efficient Multi-chained Stream Signature), provides high loss resistance, non repudiation of origin and low overhead, at the cost of slightly delayed verification. These methods including TESLA and its variants can provide message sender authentication. However, this scheme requires initial time synchronization, which is difficult to implement in large scale WSNs. They also introduce delay in message authentication, and the delay increases as the network scales up.

In several cryptographic methods [6] that have most recently been proposed for achieving several security goals in wireless sensor networks. These methods use “perturbation polynomials” to add “noise” to polynomial-based systems that provide information theoretic security, while maintaining efficiency, attempt to increase the threshold. They show that the heuristic security arguments given for these modified methods do not hold and once if they allow a slight extension of parameter then it can be completely broken.

In the paper [7], they says that in the random oracle model, where all users have access to a public random oracle. It gives a bridge between cryptographic theory and practice. In the paradigm they advise a practical protocol is produced by _rst devising and proving correct a protocol and then replacing oracle accesses by the computation of a particularly chosen function .This paradigm provides protocols more than standard ones while retaining many of the advantages of security. They demonstrate these gains for problems including signatures, encryption and zero-knowledge proofs.

Perfectly secure key distribution schemes [8] for dynamic conferences in this, a member of a group of t users ,they can compute a common key by using only his private initial piece of information and identities of the other t and one user in the group. Keys are protect against coalitions of up to k users; that means, even if k users pool together their pieces they cannot compute anything about a key of any conference comprised of t other users.

Recent progress in implementation of elliptic curve cryptography (ECC) on wireless sensors proves public key cryptography is practical for resource constrained wireless sensors. It is not straightforward due to the hardware characteristics and requirements of the wireless sensor networks [9].ECC employs a short encryption key, a value that must be input into the encryption algorithm for decoding an encrypted message. This short key is faster and requires less computing power. Now a day's both ECC and RSA are widely use. The advantages of ECC compare to RSA are more in wireless sensor devices, where storage capacity, computing power and battery backup are limited.

4. Overview of Proposed System

These above referred proposed systems are designed to authenticate the message in the network while transferring. These schemes also provide security to the messages. Following are the features of proposed system which will give desired effect.

- Elliptic curve cryptography (ECC) based authentication scheme, enabling intermediate nodes authentication and also it allows any node to transmit an unrestricted number of messages without suffering the threshold problem.
- Efficient Key managements were introduced.
- Efficient in terms of both communication and computational overhead.

4.1 Source Anonymous Message Authentication (SAMA) on Elliptic curves

SAMA generates a source anonymous message authentication for the message. SAMA scheme is a public key crypto system. The main theme is that for each m number of message to be released, the sending node or message sender generates a source anonymous message authenticator for the message m. The generation of message authentication is based on the Modified ElGamal Signature **(**MES) scheme on elliptic curves. In this scheme messages are transmitted through intermediate nodes, each intermediate node is authenticating the data whether it is modified or not. MES scheme is secure against adaptive chosen-message attacks in the random oracle model. This MES scheme enables the intermediate nodes to authenticate the message so that all unwanted message can be detected and dropped to conserve the sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection, this scheme does not have the threshold problem. The Figure 2 shows the system design of the projects. In this, implementing a source anonymous message authentication code (SAMAC) on elliptic curves. It is an efficient intermediate message authentication mechanism for WSNs without the threshold limitation. Then propose an efficient key management framework to ensure isolation of the compromised nodes.

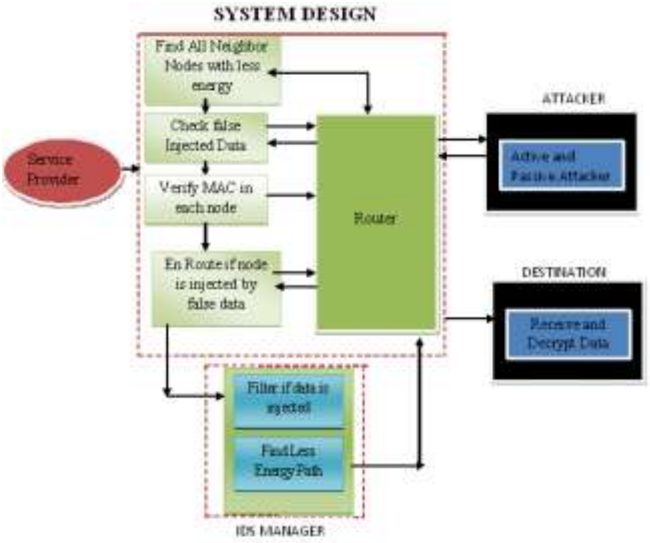
SYSTEM DESIGN
Find All Neighbor Nodes with less energy
Check false Injected Data
Service Provider
Verify MAC in each node
En Route if node is injected by false data
Router
ATTACKER
Active and Passive Attacker
DESTINATION
Receive and Decrypt Data
Filter if data is injected
Find Less Energy Path
IDS MANAGER

Figure 2: System Design

4.2 Algorithm Definition

Signature Generation Algorithm:

Input: An elliptic curve with a fixed point G on it, together with its order n, the private key $1 < d < n - 1$, the public key $R = dG$, and the message m to be signed.

Output: The pair of integers (r, s) as the signature of the message m.

```
1: Select a random integer $1 < k < n - 1$
2: Compute  $(x1, y1)=kG$ and $r = x1 \bmod n$
3: if $r = 0$ then
4: Go to 1
5: end if
6: Compute $k-1 \bmod n$
7: Compute $s = k-1(H(m) + dr) \bmod n$
8: if $s = 0$ then
9: Go to 1
10: end if
11: return (r, s)
```

Signature Verification Algorithm:

Input: An elliptic curve with a fixed point G on it, together with its order n, the public key $R = dQ$, the message m which is signed, and a pair of integers (r, s) as the signature.

Output: TRUE if (r, s) is a valid signature for m, FALSE otherwise.

```
1: Compute $c = s-1 \bmod n$ and H(m)
2: Compute $u1 = H(m) \cdot c \bmod n$ and $u2 = r \cdot c \bmod n$
3: Compute $(x0,y0)=u1Q + u2R$  and    $v = x0 \bmod n$
4: if $r = v$ then
5: Output TRUE
6: else
7: Output FALSE
8: end if
```

5. Results Analysis

Compare to the existing system, energy consumed by each node is less and time delay for routing is comparatively less.

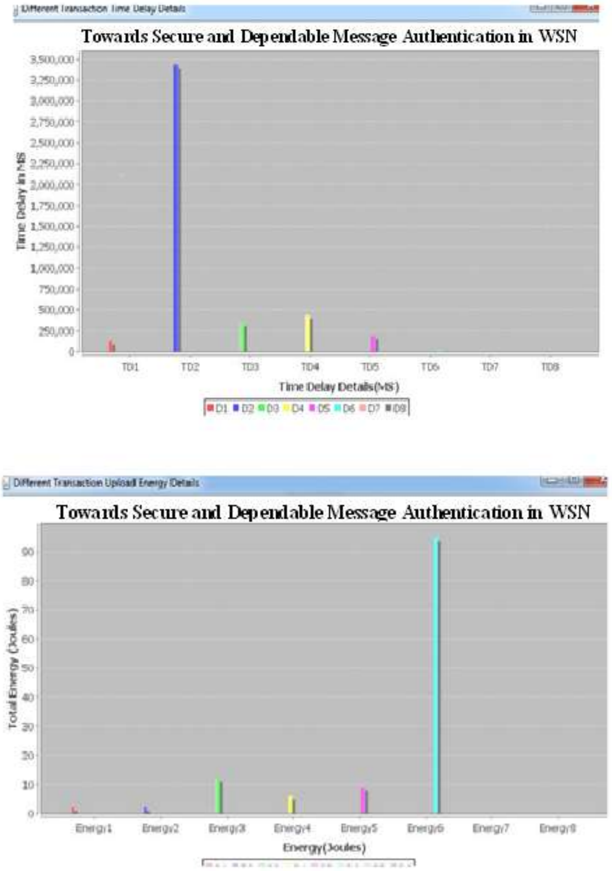

Figure 3: Energy and Time delay Details

6. Conclusions

This paper, 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 secure and dependable message authentication without the weakness of the built in threshold of the polynomial-based scheme, then proposes a secure message authentication scheme based on the SAMA. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification. This proposed scheme is more efficient than the 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] 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.

[4] 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.

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

[8] 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.

[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.