Secure and Efficient Intermediate Node Authentication in Wireless Sensor Networks

R. C. Choukimath and V. V. Ayyannavar
Dept. of Computer Science and Engineering, Basaveshwara Engineering College, Bagalkot, Karnataka, India
Email: rajeshwari.404@gmail.com; vasudha_125@rediffmail.com

***Abstract*—Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial, when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. Thus the aim of the project is to implement a scalable authentication scheme based on elliptic curve cryptography (ECC).While enabling intermediate nodes authentication. The proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, the scheme can also provide message source privacy.**

***Index Terms*—WSN, polynomial scheme, ECC**

I. Introduction

A wireless sensor network (WSN) is used to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Fig. 1 shows the scenario of wireless sensor networks. The WSN is built of "nodes" - from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs). But most of them have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial.

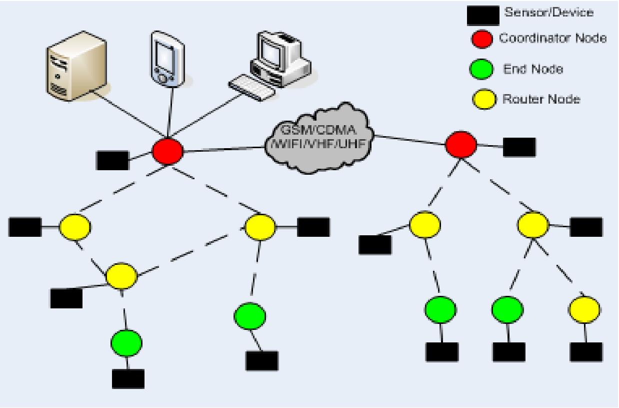


Figure 1 Scenario of wireless sensor network

This project propose a unconditionally secure and efficient source anonymous message authentication [SAMA] scheme based on the optimal modified, ElGamalsignature [MES] scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle mode. This scheme enables the intermediate nodes to authenticate the message so that all corrupted

Manuscript received June 27, 2014; revised September 22, 2014.

doi: 10.12720/ijsps.3.1.71-74

message can be detected and dropped to conserve the sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection, and also this scheme does not have the threshold problem.

A. *Existing System*

The symmetric-key based approach requires complex key management [1], lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a message authentication code (MAC) [2] for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced [3]. The idea of this scheme is similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. This approach offers information-theoretic security of the shared secret key when the number of messages transmitted is less than the threshold [4]. The intermediate nodes verify the authenticity of the message through a polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. An alternative solution was proposed in [5] to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is to add a random noise, also called a perturbation factor, to the polynomial so that the coefficients of the polynomial cannot be easily solved however, a recent study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques [6]. For the public-key based approach [7], [8], each message is transmitted 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.

B. *Issues Identified*

- In these schemes, each symmetric authentication [9] 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 [10], can also provide message sender authentication. However, this scheme requires initial time synchronization, which is not easy to be implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up.
- In polynomial scheme [11] only limited number of messages can be transmitted.

II. Problem Statement

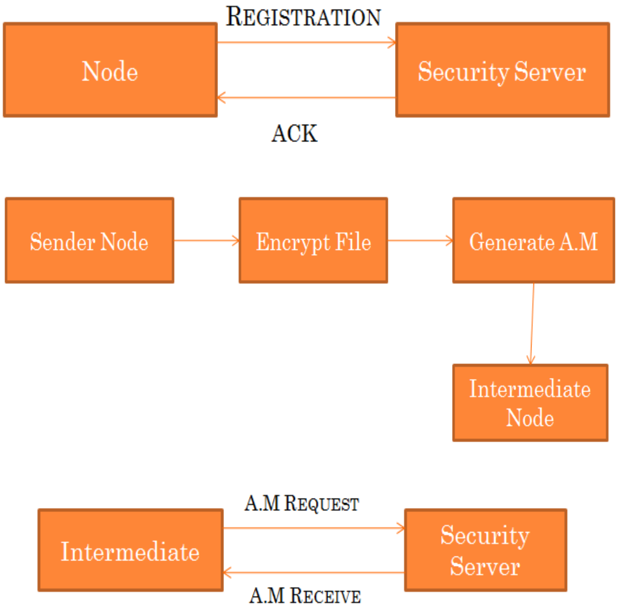
Purpose of the project is to provide intermediate node authentication without the threshold limitation, and to perform better than the symmetric-key based schemes. The distributed nature of algorithm makes the scheme suitable for decentralized networks.

Important purposes are as follows:

1) To develop a source anonymous message authentication code [12] (SAMAC) on elliptic curves that can provide unconditional source anonymity.
2) To offer an efficient intermediate node authentication mechanism for WSNs without the threshold limitation.
3) To the devise network implementation criteria on source node privacy protection in WSNs.

III. Proposed Methodology

An unconditional secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) [13] scheme on elliptic curves is implemented. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection. The Fig. 2 shows the overall architecture of the flow of the projects. In this the need of implementing a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. Then offer 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.



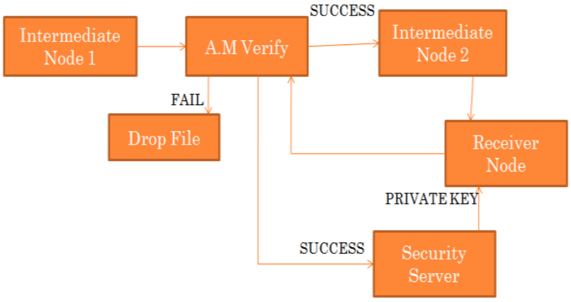


Figure 2. Block diagram of proposed work

A. Design Goals

Proposed authentication scheme aims at achieving the following goals:

- **Node authentication:** The message receiver should be able to verify whether a received message is sent by the node that is claimed, or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.
- **Message integrity:** The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.
- **Intermediate node authentication:** Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.
- **Identity and location privacy:** The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.
- **Efficiency:** The scheme should be efficient in terms of both computational and communication overhead.

IV. Results and Discussion

The Fig. 3 is a Security server (SS) that is responsible for generation, storage and distribution 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 information stored in the sensor node can be accessed by the attackers. The compromised node can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by SS and other nodes.

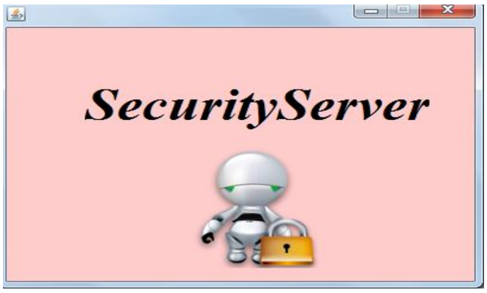
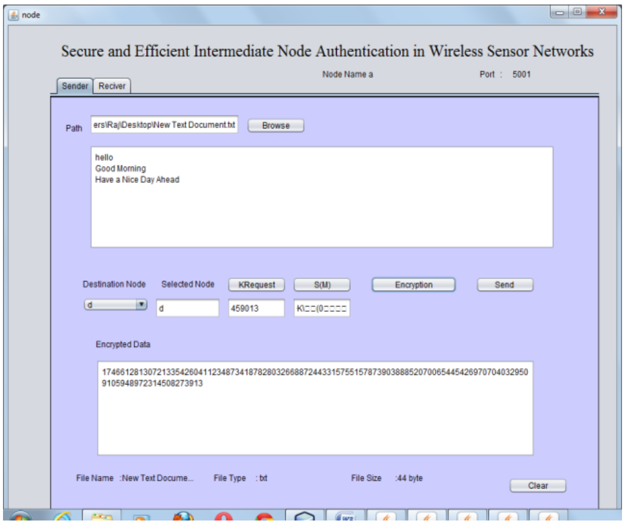


Figure 3. Security server


node
Secure and Efficient Intermediate Node Authentication in Wireless Sensor Networks
Sender
Reciver
Browse
KRequest
S(M)
Encryption
Send
Clear

Node Name a

Port : 5001

Path ers\Raj\Desktop\New Text Document.txt

hello
Good Morning
Have a Nice Day Ahead

Destination Node: d

Selected Node: d

KRequest: 459013

S(M): K\□□(0□□□□

Encrypted Data

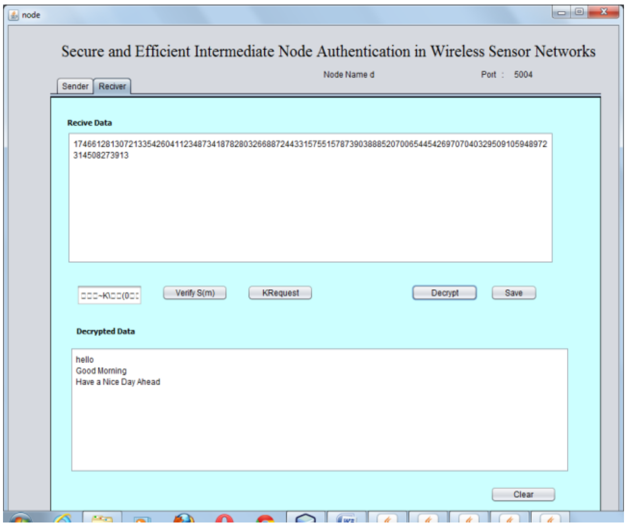
```
174661281307213354260411234873418782803266887244331575515787390388852070065445426970704032950
9105948972314508273913
```

File Name :New Text Docume... File Type : txt File Size :44 byte

Figure 4. Sender side

When the intermediate node receives the message, then it request the key to SS to verify AM, if it is same then it forwards else it will drop. When nodes gets login this window pops up, and this Fig. 4, is the sender part, first we have to browse the text file to encrypt, then choose the destination node, click on key request it generates the key, then click on S(m) to generate the anonymous message then click on Encrypt button, Thus the text field shows the encrypted message.

Once if we click on send button, then the message is sent randomly to any of the intermediate node, thus here the intermediate Node C gets the message. Once the node C receives the message we should go for the Receiver Part, which is shown in Fig. 5, then we should click on verity s(m), thus it verifies the anonymous if it is same as sent then it shows the valid source dialogue box, then click on forward button. Then the message is forwarded to the ultimate destination Node D.


node
Secure and Efficient Intermediate Node Authentication in Wireless Sensor Networks
Sender
Reciver
Verify S(m)
KRequest
Decrypt
Save
Clear

Node Name d

Port : 5004

Recive Data

```
1746612813072133542604112348734187828032668872443315755157873903888520700654454269707040329509105948972
314508273913
```

□□□~K\□□(0□□

Decrypted Data

hello
Good Morning
Have a Nice Day Ahead

Figure 5. Receiver side

At the receiver part, the text field contains the cipher text, then click on verify s(m), If the AM is same as the sent AM, then the valid source dialogue box pops up. Then click on

Key Request, thus it gets the correct key from the SS, thus finally click on Decrypt button to decrypt the message.

In between the normal scenario if the attacker login means, he browse some text and inject it to any node. The Line in the AM field indicates that the message is not from the intended source. When clicked on verify s(m), the dialogue box pops up indicating Threat Detected from the invalid source. Thus the message is dropped.

V. Conclusion

The proposed system uses a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management. For the public-key based approach, each message is transmitted 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. SAMA can be applied to any message to provide message content authenticity. In addition, our schemes enable an en-route node to detect and drop injected false data reports as early as possible, thus saving its energy that will otherwise be wasted for forwarding these false data reports. And provide intermediate message authentication without the weakness of the built in threshold of the polynomial-based scheme when applied to WSNs with fixed sink nodes.

VI. Future Work

As future work, several directions are worth investigating. In particular, we plan to address the use of interleaved Intermediate authentication for preventing or mitigating attacks against sensor network routing and data collection protocols, such as those pointed out in [Karlof and Wagner 2003]. Another topic that we plan to address is how the proposed scheme can be adapted for handling more complex data reports. Public keys should be updated periodically in order to protect the system. This update generates message exchanges between nodes and symmetric key updates.

References

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in *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," in *Proc. IEEE Symposium on 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," in *Proc. Advances in Cryptology - Crypto'92, ser. Lecture Notes in Computer Science*, 1992, pp. 471-486.

[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise resilient message authentication in sensor networks," in *Proc. IEEE INFOCOM*, Phoenix, AZ., Apr. 15-17, 2008.

[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symposium on Security and Privacy*, May 2000.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on perturbation polynomials," Cryptology ePrint Archive, Report 2009/098, 2009.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Assoc. of Comp. Mach.*, 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 Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 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," in *Proc. IEEE ICDCS*, Beijing, China, 2008, pp. 11-18.

[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," *Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science*, vol. 1070, pp. 387-398, 1996.

[11] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the Assoc. of Comp. Mach.*, vol. 24, no. 2, pp. 84-88, Feb. 1981.

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

[13] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361-396, 2000.

Miss Rajeshwari C. Choukimath was born on 30th sept 1989, Bagalkot, Karnataka, India. She is currently perceiving her PG degree in Computer Science and Engineering College Bagalkot-587102. Her research interests include wireless sensor networks, Cloud computing.

Mrs. V. V. Ayyannavar was born on 11th June 1981, Bagalkot, Karnataka, India. She has perceived her M.Tech from VTU University. She is currently working as an Asst. Professor in Computer Science and Engineering College Bagalkot-587102, Karnataka, India. Her research interest is Networking.