Multiple Node Message Authentication and Source Privacy in Wireless Sensor Networks

A. Mummoorthy[1], G. Dilip Pious Joe[2], K. Sulaiman Mydeen[3], M. Aravinth[4], A. Lakshmana Kumar[5]
[1, 2, 3, 4, 5] Department of CSE
[1, 2, 3, 4, 5] K.S.R college of Engineering, Tiruchengode

Abstract- *Message Sources Anonymity Message authentication is providing various services such as confidentiality, integrity, protection of privacy in wireless sensor network. Message authentication schemes can largely be divided into two methodologies: public-key based and symmetric-key based approaches. The symmetric-key based approach requires complex key management, lacks of scalability, and is not flexible to large numbers of node negotiation attacks since the message sender and the receiver have to share a secret key. However, both symmetric and public-key methods 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, this paper describes 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. In addition paper, the GECC scheme can also provide message source privacy and also multiple base station environments are considered.*

Keywords- MSAM, Key Management, ECC, GECC, Message Verification.

I. INTRODUCTION

Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication in future. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless sensor networks (WSN) are currently receiving significant attention due to their unlimited potential. However, it is still very early in the lifetime of such systems and many research challenges exist. In this thesis works the security aspects of these networks.

II. EXISTING SYSTEM

The existing system develops a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. It offers an efficient multiple node message authentication mechanism for WSNs without the threshold limitation. It devises network implementation criteria on source node privacy protection in WSNs. It proposes an efficient key management framework to ensure isolation of the compromised nodes.

III. PROPOSED SYSTEM

Propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to con- serve the sensor power. While makes it lucrative for being exploited in abundance resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based algorithms under comparable security levels To verify whether a received message is sent by the node that is claimed or by a node in a particular group.

Multiple node message 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.

Message is generated like the following:

Generate (m, PQ1, PQ2,..., PQn). Given a message m and the public keys PQ1, PQ2,..., PQn of the AS (Ambiguous Set) S={A1,A2, ... ,An}, the actual message sender At, 1 <= t <= n, produces an anonymous message S(m) using its own private key dt.

Verify S(m). Given a message m and an anonymous message S(m), which includes the public keys of all members in the

AS, a verifier can determine whether S(m) is generated by a member in the AS.

The security requirements include:

Sender ambiguity: The probability that a verifier successfully determines the real sender of the anonymous message is exactly 1=n, where n is the total number of members in the AS.

Unforgetability: An anonymous message scheme is unforgetable if no adversary, given the public keys of all members of the AS and the anonymous messages m_1, m_2,..., m_n adaptively chosen by the adversary, can produce the message.

The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS.

Suppose that the message sender (say Alice) wishes to transmit a message m anonymously from her network node to any other nodes. The AS includes n members, A1,A2, ... ,An, for example, S={A1,A2, ... ,An}, where the actual message dropped to con- serve the sensor power. While achieving compromise- this project, we will not distinguish between the node Ai and its public key PQi. Therefore, we also haveS= {PQ1,P Q2, ...,PQn}.

IV. MESSAGE GENERATION IN SOURCE NODE

In this methodology, the message is generated in source node. The message receiver should be able

Authentication generation algorithm: Suppose m is a message to be transmitted along with base station node id. The private key of the message sender Alice is dt; 1 <= t <= n. To generate an efficient scheme for message m, Alice performs the following three steps:

1. Select a random and pairwise different ki for each $1 \leq 0$ $i \leq 0\ n-1, i \neq 0\ t$ and compute ri from (ri,yi) = k_iG.
2. Choose a random ki$\in$0 Zp and compute r_t from (rt, yt)= k_tG - $\sum i\neq 0t0\ r_ih_{iP}Q_i$ such that $r_t \neq 0$ and $r_t \neq r_i$ for any i <> t, where $h_i = h(m, r_i)$.
3. Compute $s = k_t + \sum_{t\neq t}0k_i + r_td_th_t \bmod N$.

The scheme of the message m is defined as:

S(m) = (m, S, r1, y1, ... , r_n, y_n, s).

V. MESSAGE VERIFICATION IN SINK NODE OR BASE STATION

Verification algorithm: For Bob to verify the scheme (m, S, r1, y1, ... , r_n, y_n, s), he must have a copy of the public keys Q1, ... ,Qn. Then he:

1. Checks that $PQ_i \neq O$, i = 1, …., n otherwise invalid.
2. Checks that PQ_i, i = 1, …., n lies on the curve.
3. Checks that $nPQ_i = O$, i = 1, …., n.

After that, Bob follows these steps:

1. Verify that ri, yi, i = 1,….n and s are integers in [1, N -1]. If not, the signature is invalid.
2. Calculate $h_i = h(m, r)$, where h is the same function used in the signature generation.
3. Calculate $(x0, y0) = sG - \sum_{i=1}^{n} rih_iQ_i$
4. The signature is valid if the first coordinate of $\square_i$ (ri, yi) equals x_0. invalid otherwise.

sender Alice is At, for some value t; 1 <= t <= n. In generated without being modified, then we compute:

$$
\begin{aligned}
(x_0, y_0) &= sG - \sum_{i=1}^{n} r_i h_i Q_i \\
&= \left(k_t + \sum_{i\neq t} k_i + r_t d_t h_t\right) G - \sum_i r_i h_i Q_i \\
&= \sum_{i\neq t} k_i G + \left(k_t G - \sum_{i\neq t} r_i h_i Q_i\right) \\
&= \sum_{i\neq t} (r_i, y_i) + (r_t, y_t) \\
&= \sum_i (r_i, y_i).
\end{aligned}
$$

Therefore, the verifier should always accept the Scheme.

VI. EXPERIMENTAL RESULT

Provided the training data collected during the offline training phase, we can further improve the performance of determining the number of spoofing attackers. In addition, given several statistic methods available to detect the number of attackers, such as System Evolution and combine the characteristics of these methods to achieve a higher detection rate.

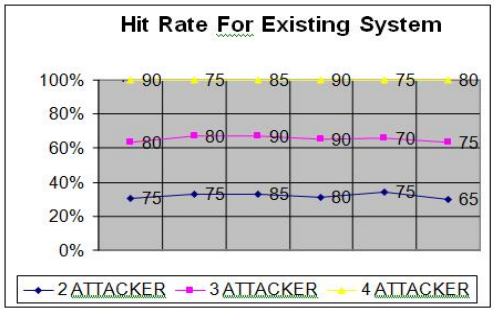
In this section, we explore using hypothesis testing to classify the number of the spoofing attackers. The advantage of using hypothesis is that it can combine the intermediate results (i.e., features) from different

statistic methods to build a model based on training data to accurately predict the number of attackers.

HIT RATE %	HIT RATE EXISTING SYSTEM	HIT RATE PROPOSED SYSTEM
75	80	90
75	80	75
85	90	85
80	90	90
75	70	75
65	75	80

The training data set can be obtained through regular network monitoring activities. Given a training set of instance-label pairs and the label, the support vector machines require the solution of the following optimization problem:

In fact, if the scheme has been correctly

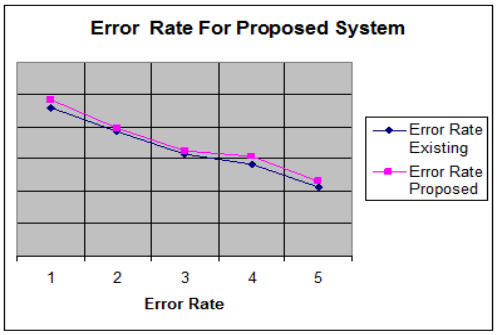


$$\min_{\mathbf{w},b,\xi} \ \frac{1}{2}\mathbf{w}^T\mathbf{w} + \mathcal{C}\sum_{i=1}^{l}\xi_i$$
$$\text{Subject to } \ y_i(\mathbf{w}^T\phi(x_i) + b) \geq 1 - \xi_i,$$
$$\xi_i \geq 0.$$

Its dual is

$$\min_{\alpha} \ \frac{1}{2}\alpha^T Q\alpha - \mathbf{e}^T\alpha$$
$$\text{Subject to } \ \mathbf{y}^T\alpha = 0,$$
$$0 \leq \alpha_i \leq C, \quad i = 1, \ldots, l,$$

VII. ERROR RATE FOR PROPOSED SYSTEM



VIII. CONCLUSION

In this paper proposed to use message sending, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting multiple attackers in wireless networks. It provided theoretical analysis of using the multiple node based inherited from wireless nodes for attack detection. The approach can both detects the presence of attacks as well as determine the number of adversaries we can localize any number of attackers and eliminate them. In addition, a Multi hop-based node message sending and compromise detection scheme is proposed using the Geometrical elliptic curve cryptography (GECC).Furthermore, several possible attacks are described against the proposed scheme and proposed multi hop based measures against these attacks. The scheme is evaluated in simulation under various scenarios. The experimental results show that the scheme quickly detects untrustworthy multi hop with a small number of trust reports. In future, the scheme may evaluate against various types of attacker models. It is believed that a game theoretic model is suited for this evaluation. A variety of strategies may be studied that may be taken by detector and adversary.

REFERENCES

[1] W. Du, J. Deng, Y. Han, and P. Varshney. A Pair wise Key Pre-distribution Scheme for Wireless Sensor Networks. In Proc. of 10th ACM Conference on Computer and Communications Security (CCS), Washington DC, October 27-31, 2003.

[2] D. Liu and P. Ning. Establishing Pair wise Keys in Distributed Sensor Networks. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., October, 2003.

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

[4] R. Blom. An Optimal Class of Symmetric Key Generation Systems. Advances in Cryptology, EUROCRYPT'84, LNCS 209, 335338, 1984.

[5] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In Advances in Cryptology CRYPTO 92, LNCS 740, pages 471486, 1993.

[6] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks," IEEE Infocom'04, March 2004.

[7] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in ACM CCS, 2002.

[8] 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.

[9] D. Liu and P. Ning. Establishing Pair wise Keys in Distributed Sensor Networks. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., October, 2003.

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

[11] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Computer, October 2003.