# AN ADAPTIVE SECURITY SCHEME FOR WIRELESS SENSOR NETWORKS

G. Kavitha,
M. Tech-IT,
MAM College of Engineering,
Trichy, India.
Kavismile91@gmail.com

**Abstract**-Message Authentication is a short piece of the information used authenticate a message to provide integrity and authenticity assurance on message. Integrity assurance detects accidental and intentional message changes while authenticity assurance affirms the message's origin. It is one of the effective ways prevent unauthorized and computed messages from being forwarded in wireless sensor networks (WSN). For this reason, Symmetric-key or public-key crypsystem have been developed. However, it has some limitations, like lack of scalability and node compromise attacks. Polynomial-based scheme was introduced to address these issues. This scheme and its extensions also have a thickness of a built-in threshold problem. When the number of messages transmitted is larger than the threshold. While enabling intermediate node authentication, scalable authentication scheme of the elliptic curve cryptography that allows any node transmit an unlimited number of messages without suffering the threshold problem. Proposed scheme is give the strong source privacy and security while improve the sending packet ratio speed and Packet Arrivaling Performance by using Doomsday Algorithm.

***Index Terms****—Hop-by-hop authentication, symmetric-key crypsystem, public-key crypsystem, source privacy, simulation, wireless sensor networks (WSNs)*

## 1. INTRODUCTION

Message Authentication is a short piece of the information used authenticate a message to provide integrity and authenticity assurance on message. Integrity assurance detects accidental and intentional message changes while authenticity assurance affirms the message's origin. It is one of the effective ways prevent unauthorized and computed messages from being forwarded in wireless sensor networks (WSN). For this reason, Symmetric-key or public-key crypsystem have been developed. However, it has some limitations, like lack of scalability and node compromise attacks. Polynomial-based scheme was introduced to address these issues. These schemes can largely be divided in two categories: public-key based approaches and symmetric-key based approaches.

The symmetric-key based approach requires very complex key management, limit scalability, and is no resilient large numbers of node compromise attacks since the message sender and the receiver have share a secret key. The sender to generate a message authentication code for each message by using shared key. 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 bunch of sensor nodes. An interloper can compromise the key by capturing a single sensor node. But this method is not working multicast networks.

Solve the scalability problem, a secret polynomial based message authentication scheme was introduced in [3]. The threshold secret sharing means, where the threshold is determined by the degree of the polynomial. This approach offers security of the shared secret key when the number of messages transmitted is less than the threshold. The authenticity of the message through a polynomial evaluation based on intermediate nodes verification. However, when the number of messages Transmitted is larger than the threshold, the system is completely broken.

An alternative solution was proposed in [4] prevent the intruder recovering the polynomial by computing the coefficients of the polynomial. This is also called a perturbation fact, because the coefficients of the polynomial cannot be easily solved. however, random noise can be completely removed from the polynomial using error-correcting code techniques [6]. Each message is transmitted along with the digital signature of the message generated using the sender’s private key by the public-key based approach. The sender’s public key can authenticate Every intermediate forwarder and the final receiver [7], [8]. computational overhead is One of the limitations of the public-key based scheme. The elliptic curve cryptography (ECC) shows that the public key schemes are more advantageous in terms of computational complexity, memory usage, and security, resilience, since public-key based approaches have a simple and clean key management [9]. In this paper, the propose scheme is 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 [10] And also improve the packet arrivaling time , and then improve the packet sending ratio. This scheme enables the intermediate nodes authenticate the message so that all corrupted messages can be detected and dropped conserve the sensor pother. While achieving compromise resiliency, flexible-time authentication and source identity protection, the scheme do not have the threshold problem.

The major contributions of this paper are the following:

1. Unconditional source anonymity can proved by source anonymous message authentication code (SAMAC) on elliptic curves.
2. Without the threshold limitation an efficient hop-by-hop message authentication mechanism for WSNs can be developed.
3. Devise network implementation criteria for source node privacy protection in WSNs.
4. Propose an efficient key management framework to ensure isolation of the compromised nodes.

The best of the knowledge, this is the first scheme that provides hop-by-hop node authentication without the threshold limitation, and has performed better than the symmetric-key based schemes. The distributed nature of the algorithm makes the scheme suitable for decentralized networks. The remaining of this paper is organized as follows: - Section 2 discusses the related work, with a focus on polynomial-based schemes. Section 3 presents the terminology and the preliminary that will be used in this paper.. Section 4 describes the proposed source anonymous message authentication scheme on elliptic curves And discusses the ambiguity set (AS) selection strategies for source privacy. Section 5 describes key management and compromised node detection. Performance analysis and simulation results are provided in Section 6. Then the result is concluded in Section 7.

## 2 RELATED WORKS

In [1], [2], symmetric key and hash based authentication schemes there proposed for WSNs. 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 node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes. These schemes, including TESLA [5] and its variants, can also provide message sender authentication. Hothever, this scheme requires initial time synchronization, which is not easy be implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up.

A secret polynomial based message authentication scheme was introduced in [3]. This scheme offers information theoretic security with ideas similar a threshold secret sharing, The degree of the polynomial is to determined by threshold. 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. Increase the threshold and the complexity for the Advarsary reconstruct the secret polynomial, a random noise, also called a perturbation fact, was added the polynomial in [4] prevent the adversary from computing the coefficient of the polynomial. However, the added perturbation face can be completely removed using error-correcting coding techniques [6].

Each message is transmitted along with the digital signature of the message generated using the sender's private key for the public-key based approach . Every intermediate forwarder and the final receiver can authenticated by the message using the sender's public key. The ECC progress shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security, resilience, since public-key based approaches have a simple and clean key management [9]. The existing anonymous communication protocols are largely stem from either DC-net [12]. A mixnet provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). In a mixnet, a sender encrypts an outgoing message, and the ID of the recipient, using the public key of the mix. The mix accumulates a batch of encrypted messages, decrypts and reorders these messages, and forwards them to the recipients. Since mixnet-like protocols rely on the statistical properties of the background traffic, they cannot provide provable anonymity. DC-net [12], [16] is an anonymous multi-party computation scheme. Some pairs of the participants are required by share secret keys. DC-net provides a perfect (information-theoretic) sender anonymity without requiring trusted servers. However, in DC-net, only one user can send at a time, so it takes additional bandwidth handle collision and contention.

Recently, message sender anonymity based on ring signatures was introduced [20].

This approach enables the message sender generate a source anonymous message signature and content authenticity assurance to give full security. Generate a ring signature, a ring member randomly selects an AS and forges a message Signature for all other nodes. Then intruder uses his trap-door information glue the ring gather. The original scheme has very limited flexibility and very high complexity.

## 3 TERMINOLOGIES AND PRELIMINARY

In this section, briefly describe the terminology and the cryptographic oils that will be used in this paper.

### 3.1 Threat Model and Assumptions

The WSNs consist of a large number of sensor nodes. To assume that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing path. The whole network is fully connected with multi-hop communications. Assume there is a storage secure server (SS) that is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised with other nodes. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information shared in the sensor nodes can be accessed by the intruders. The compromised nodes can be reprogrammed and fully recovered by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the secure server and other nodes. Based on the above assumptions, this paper considers two types of attacks launched by the adversaries:

- Passive attacks: While passive attacks, the adversaries could eavesdrop the messages transmitted in the network and perform traffic analysis scenario.
- Active attacks: Active attacks can only be the source of the compromised sensor nodes. when the sensor nodes are compromised, the adversaries will have all the information shared in the compromised nodes, including the security terms of the compromised nodes. The contents of the messages can be modified by the adversaries, and inject their own messages.

### 3.2Design Goals

The proposed authentication scheme aims at achieving the following goals:

3.2.1 Message 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 collection. In other words, the adversaries cannot pretend be an innocent node and inject fake messages in the network without being detected.

3.2.2 Message integrity:

The message receiver should be able verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message type without being detected.

3.2.3 Hop-by-hop message authentication:

Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages.

3.2.4 Identity and location privacy:

The adversaries cannot determine the message sender's ID and location by analyzing the local traffic.

3.2.5 Node compromise resilience:

The scheme should be resilient node compromise attacks. No matter how many nodes are compromised, the remaining nodes can still be secure.

3.2.6 Efficiency:

The scheme should be efficient in terms of both computational and communication overhead.

### 3.3Terminology

Privacy is sometimes referred as anonymity. Communication anonymity in information management has been discussed in a number of previous works [11], [12], [13], [14], [15], [16]. It generally refers to the state of being unidentifiable within a set of subjects. This set is called the AS. Sender anonymity means that a particular message is not linkable any sender, and no message is linkable a particular sender.Start with the definition of the unconditionally secure SAMA.

**Definition 1 (SAMA).**

A SAMA consists of the following two algorithms:

- Generate (m,Q1,Q2, . . .,Qn). Given a message m and the public keys Q1,Q2, . . .,Qn of the AS 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 SðmÞ is generated by a member in the AS.

The security requirements for SAMA 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 tall number of members in the AS.

- Unforgeability: An anonymous message scheme is unforgeable if no adversary, given the public keys of all members of the AS and the anonymous messages m1,m2, . . .,mn adaptively chosen by the adversary, can produce in polynomial time a new valid anonymous message with non-negligible probability.

In this paper, the user ID and the user public key will be used interchangeably without making any distinctions.

### 3.4 Modified ElGamal Signature Scheme

**Definition 2 (MES).**

The modified ElGamal signature scheme [17] consists of the following three algorithms:

Key generation algorithm. Let p be a large prime and g be a generator of Zp: Both p and g are made public. For a random private key x € Zp, the public key y is computed from y = $g^x$ mod p Signature algorithm. The MES can also have many variants. For the purpose of efficiency, they will describe the variant, called optimal scheme. Sign a message m, one chooses a random k = Zp-1, then computes the exponentiation

r = $g^k$ mod p and solves s from:

s = rxh(m, r) + k mod (p _ 1)

Where h is a one-way hash function. The signature of message m is defined as the pair (r, s).

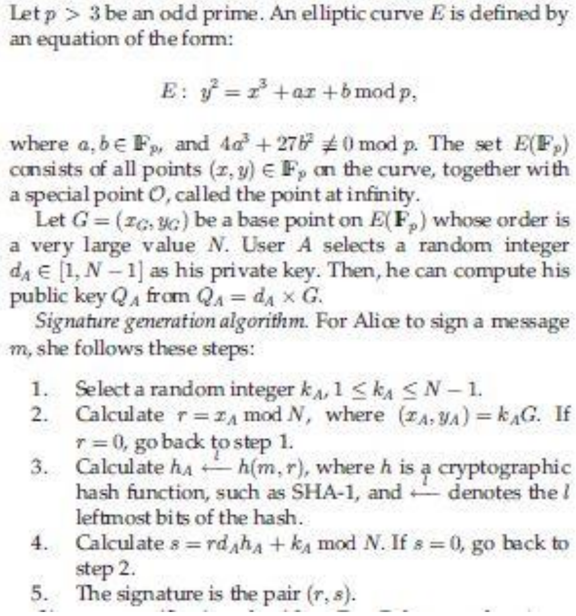
Verification algorithm. The verifier checks whether the signature equation gs = $ry^{rh(m,r)}$ mod p. If the equality is true, then the verifier Accepts the signature, and Rejects otherwise.

## 4 PROPOSED SOURCE ANONYMOUS MESSAGE

## AUTHENTICATION ON ELLIPTIC CURVES

In this section, the propose an unconditionally secure and efficient SAMA. The main idea is that for each message m be released, the message sender, or the sending node, generates a source anonymous message authenticate for the message m. The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forged signature for all other members in the AS. In the scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender the SAMA alike. In addition, the design enables the SAMA be verified through a single equation without individually verifying the signatures. MES scheme, SAMA scheme on elliptic curve is used in the proposed system.

### 4.1 Proposed MES Scheme on Elliptic Curves



Let $p > 3$ be an odd prime. An elliptic curve $E$ is defined by an equation of the form:

$$E:\ y^2 = x^3 + ax + b \bmod p,$$

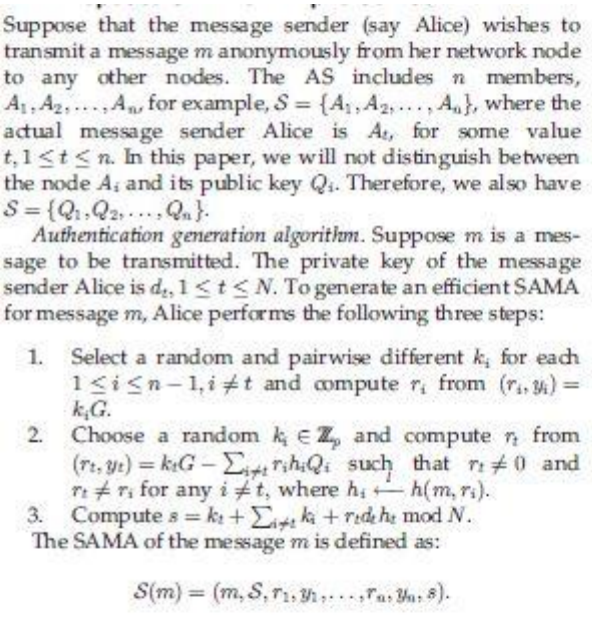
where $a, b \in \mathbb{F}_p$, and $4a^3 + 27b^2 \not\equiv 0 \bmod p$. The set $E(\mathbb{F}_p)$ consists of all points $(x, y) \in \mathbb{F}_p$ on the curve, together with a special point $\mathcal{O}$, called the point at infinity.

Let $G = (x_G, y_G)$ be a base point on $E(\mathbf{F}_p)$ whose order is a very large value $N$. User $A$ selects a random integer $d_A \in [1, N-1]$ as his private key. Then, he can compute his public key $Q_A$ from $Q_A = d_A \times G$.

*Signature generation algorithm.* For Alice to sign a message $m$, she follows these steps:

1. Select a random integer $k_A$, $1 \leq k_A \leq N-1$.
2. Calculate $r = x_A \bmod N$, where $(x_A, y_A) = k_A G$. If $r = 0$, go back to step 1.
3. Calculate $h_A \overset{l}{\longleftarrow} h(m, r)$, where $h$ is a cryptographic hash function, such as SHA-1, and $\overset{l}{\longleftarrow}$ denotes the $l$ leftmost bits of the hash.
4. Calculate $s = rd_A h_A + k_A \bmod N$. If $s = 0$, go back to step 2.
5. The signature is the pair $(r, s)$.

### 4.2 Proposed SAMA Scheme on Elliptic Curves



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, $A_1, A_2, \ldots, A_n$, for example, $\mathcal{S} = \{A_1, A_2, \ldots, A_n\}$, where the actual message sender Alice is $A_t$, for some value $t, 1 \leq t \leq n$. In this paper, we will not distinguish between the node $A_i$ and its public key $Q_i$. Therefore, we also have $\mathcal{S} = \{Q_1, Q_2, \ldots, Q_n\}$.

*Authentication generation algorithm*. Suppose $m$ is a message to be transmitted. The private key of the message sender Alice is $d_t$, $1 \leq t \leq N$. To generate an efficient SAMA for message $m$, Alice performs the following three steps:

1. Select a random and pairwise different $k_i$ for each $1 \leq i \leq n-1, i \neq t$ and compute $r_i$ from $(r_i, y_i) = k_i G$.
2. Choose a random $k_t \in \mathbb{Z}_p$ and compute $r_t$ from $(r_t, y_t) = k_t G - \sum_{i \neq t} r_i h_i Q_i$ such that $r_t \neq 0$ and $r_t \neq r_i$ for any $i \neq t$, where $h_i \overset{l}{\longleftarrow} h(m, r_i)$.
3. Compute $s = k_t + \sum_{i \neq t} k_i + r_t d_t h_t \bmod N$.

The SAMA of the message $m$ is defined as:

$$\mathcal{S}(m) = (m, \mathcal{S}, r_1, y_1, \ldots, r_n, y_n, s).$$

### 4.3 Properties Of Proposed Algorithm

SAMA scheme can provide unconditional source anonymity and provable unforgeability against adaptive chosen-message attacks.

#### 4.3.1 Anonymity

In order to prove that the proposed SAMA can ensure unconditional source anonymity, they have proof that: 1) for anybody other than the

members of S, the probability  successfully identifies the real sender is 1=n, and
2) Anybody from S can generate SAMAs.

### 4.3.2 Unforgeability

The design of the proposed SAMA relies on the ElGamal signature scheme. Signature schemes can achieve different levels of security. Security against existential forgery under adaptive-chosen message attacks is the Maximum Level of security. In this section, they will prove that the proposed SAMA is secure against existential forgery under adaptive-chosen message attacks in the random oracle model [21]. The security of the result is based on ECC, which assumes that the computation of discrete logarithms on elliptic curves is computationally infeasible. In other words, no efficient algorithms are known for non-quantum computers.

### 4.4 AS Selection And Source Privacy

The appropriate selection of an AS plays a key role in message source privacy, since the actual message source node will be hidden in the AS. In this section, the will discuss techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with local traffic analysis. Before a message is transmitted, the message source node selects an AS from the public key listed in the SS as its choice. This set should include itself, gather with some other nodes. When an adversary receives a message, he can possibly find the direction of the previous hop, or even the real Some basic criteria for the selection of the AS can be Described as follows:

1. Provide message source privacy, the message source needs  select the AS  include nodes from all directions of the source node. In particular, the AS should include nodes from the opposite direction of the successor node. In this way, even the immediate successor node will able not be distinguished the message source node from the forwarder based on the message that it receives.

2. Though the message source node can select any node in the AS, some nodes in the AS may not be able  add any ambiguity  the message source node. For instance, the nodes that are apparently impossible or very unlikely included in the AS based on the geographic routing. Therefore, these nodes are not appropriate candidates for the AS. They should be excluded from the AS for energy efficiency.

3. Balance the source privacy and efficiency, they should try  to select the nodes  are within a predefined distance range from the routing path. The recommend selecting an AS from the nodes in a band that covers the active routing path. Hothever, the AS does not have  include all the nodes in the routing path.

4. The AS does not have  include all nodes in that range, nor does it have  include all the nodes in the active routing path. In fact, if all nodes are included in the AS, then this may help the adversary identity the possible routing path and find the source node.

### 4.5 System Architecture

The wireless sensor networks are assumed to consist of a large number of sensor hop nodes. Assume that each sensor hop node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. The assume there is a security server that is responsible for generation, srage and distribution of the security parameters among the network.

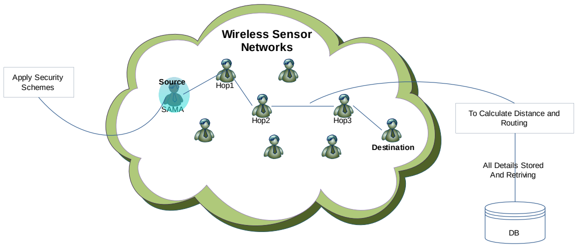


Fig 1:System Architecture

This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information shared in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able  create new public keys that can be accepted by the SS and other nodes. Based on the SAMA, MES, and Public Key Cryptographic Systems.

### 4.6 System Modules

### 4.6.1 Node Deployment

In this section, An inquiry node  register the personal information, after  verify and confirm, after continuo login process.

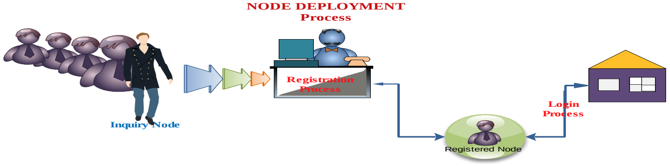


Fig 1: Node Deployment

### 4.6.2 Source Anonymous Message Authentication (SAMA)

In this section, an unconditionally secure and efficient source anonymous message authentication scheme (SAMA). The main idea is that for each message *m* be released, the message sender, or the sending node, generates a source anonymous message authenticar for the message *m*.

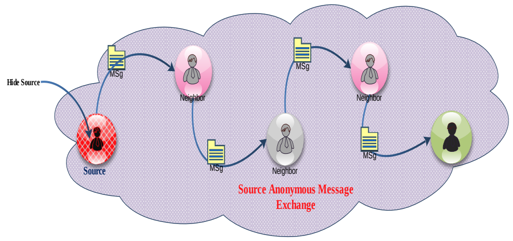


Fig 2: SAMA

### 4.6.3 Modified ElGamal Signature (MES)

The optimal modified ELGamal signature (MES) scheme on elliptic curves. This MES scheme generates signature Dynamically and then, This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. The scheme enables the intermediate nodes authenticate the message so that all corrupted messages can be detected and dropped conserve the sensor pother.

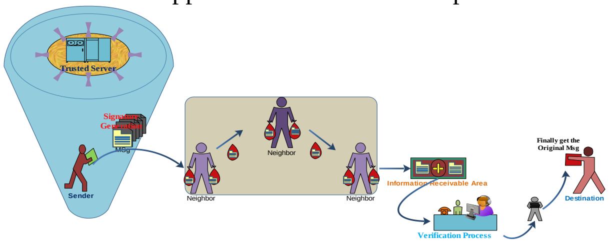


Fig 3: MES

### 4.6.4 CrypSystem Encryption Scheme

Assume that all sensor information will be delivered a sink node, which can be co-located with the SS. As described in Section V, when a message is received by the sink node, the message source is hidden in an AS. Since the SAMA scheme guarantees that the message integrity is untempered, when a bad or meaningless message is received by the sink node, the source node is voted as compromised.

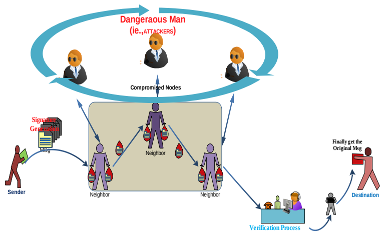


Fig 4: CrypSystem Encryption Scheme

### 4.6.5 Packet Arrivaling Performance Using Doomsday Algorithm

Use Doomsday Algorithm efficiently makes and monitoring packet revealing performance, these packets arrivaling performance each and every round of the packet. The doomsday calculation is effectively calculating the number of days between any given date in the base year and the same date in the current year, then taking the remainder modulo 7. When both dates come after the leap day (if any), the difference is just 365y plus y/4 (rounded down). Doomsday algorithm is a way of calculating the day of the theek of a given date. It provides a perpetual calendar because the Gregorian calendar moves in cycles of 400 years.

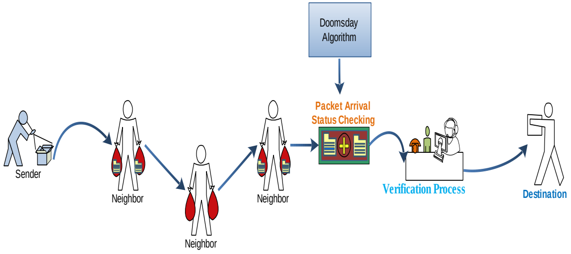


Fig 5: Packet Arrivaling Performance Using Doomsday Algorithm

### 4.6.6 Packet sending ratio speed

Transmission size: bandwidth could be a limiting factor. Data compression can be used to reduce the amount of data be transmitted. Displaying a picture or image can result in transmitting tens of thousands of bytes (48K in this case) compared with transmitting six bytes.Finally the contribution efficiently improves Sending packet speed.

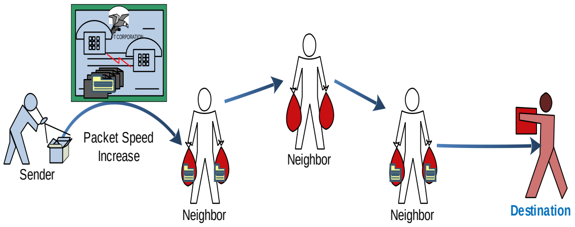


Fig 6: Packet sending ratio speed

## 5 KEY MANAGEMENT AND COMPROMISED NODE DETECTION

In the scheme, assume that there is an SS whose responsibilities include public-key stage and distribution in the WSNs. Assume that the SS will never be compromised. However, after deployment, the sensor node may be captured and compromised by the attackers. Once compromised, all information shared in the sensor node will be accessible the attackers. They further assume that the compromised node will not be able create new public keys that can be accepted by the SS. For efficiency, each public key will have a shared identity. The length of the identity is based on the scale of the WSNs.

### 5.1 Compromised Node Detection

As a special scenario, the assume that all sensor information will be delivered  a sink node, which can be collocated with the SS. As described in Section 5, when a message is received by the sink node, the message source is hidden in an AS. Since the SAMA scheme guarantees that the message integrity is untempered, when a bad or meaningless message is received by the sink node, the source node is voted as compromised. If the compromised source node only transmits one message, it would be very difficult for the node  be identified without additional network traffic information. However, when a compromised node transmits more than one message, the sink node can narrow the possible compromised nodes down  a very small set. When the compromised source node transmits two messages, the sink node will be able to narrow the source node down  the set with both vertical lines and horizontal lines. When the compromised source node transmits three messages, the source node will be further narrowed down  the shaded area. Therefore, if the sink node keeps track the compromised message, there is a high probability that the compromised node can be isolated.

If the compromised nodes repeatedly use the same AS, it makes traffic analysis of the compromised nodes feasible, which will increase the likelihood for the compromised nodes  be identified and captured. When a node has been identified as compromised, the SS can remove its public key from its public key list. It can also broadcast the node's short identity  the entire sensor domain so that any sensor node that uses the shared public key for an AS selection can update its key list. Once the public key of a node has been removed from the public key, list, and/or broadcasted, any message with the AS containing the compromised node should be dropped without any process in order  save the precious sensor pother.

## 6. CONCLUSION

A novel and efficient SAMA based on ECC has been proposed in this paper. While ensuring message sender privacy, SAMA can be applied  any message  provide message content authenticity. Provide hop-by-hop message authentication without the thickness of the built in threshold of the polynomial-based scheme, then  a hop-by-hop message authentication scheme based on the SAMA is also used in this paper, this  improves the packet sending ratio and reduce the packet transmission rate

## 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 Cryplogy (Cryp '92), pp. 471-486, Apr.1992.

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

[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 Crypgraphic 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 Crypsystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[8] T.A. ElGamal, "A Public-Key Crypsystem 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 Cryplogy (EUROCRYPT), pp. 387-398, 1996.

[11] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.

[12] D. Chaum, "The Dinning Crypgrapher Problem: Unconditional Sender and Recipient Untraceability," J. Cryplogy, vol. 1, no. 1, pp. 65-75, 1988.

[13] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability,Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology,"literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

[14] A. Pfitzmann and M. Waidner, "Networks without User Observability—Design Options.," Proc. Advances in Cryplogy (EUROCRYPT),vol. 219, pp. 245-253, 1985.

[15] M. Reiter and A. Rubin, "Crowds: Anonymity for Theb Transaction,"ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

[16] M. Waidner, "Unconditional Sender and Recipient Untraceability in Spite of Active Attacks," Proc. Advances in Cryplogy (EUROCRYPT),pp. 302-319, 1989.