IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
www.ijiset.com
ISSN 2348 – 7968

An Improved and Trustworthy Communication Framework in Wireless Sensor Network's

P.Venkata Kiranmai[1] M.Sreenivasulu[2]

[1] Department of CSE, J.N.T.U Anantapur, Tirupathi, Andhra Pradesh, India,Email-mai100.kiran@gmail.com

[2] Department of CSE, Sathyabama University, Chennai, Tamilnadu,India,Email-srm200546@gmail.com

Abstract

Message authentication is one in all the foremost effective ways in which to thwart unauthorized and corrupted messages from being forwarded in wireless device networks (WSNs). For this reason, several message authentication schemes are developed, supported either symmetric-key cryptosystems or public-key cryptosystems. Polynomial-based theme was recently introduced. However, this theme and its extensions all have the weakness of an intrinsic threshold determined by the degree of the polynomial once the amount of messages transmitted is larger than this threshold. During this paper, we propose to scalable authentication theme supported elliptic curve cryptography (ECC). Whereas sanctionative intermediate nodes authentication, our planned theme permits any node to transmit a vast variety of messages while not suffering the edge drawback. Additionally, our theme also can give message supply privacy. Each theoretical analysis and simulation results demonstrate that our planned theme is a lot of economical than polynomial-based approach in terms of process and communication.

Keywords: *SHA, SAMA, Message Authentication, WSN, Public-Key Consumption.*

1. Introduction

MESSAGE authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save lots of the valuable sensing element energy .For this reason, several authentication schemes have been proposed in literature to supply message authenticity and integrity verification for wireless sensing element networks (WSNs). These schemes will for the most part be divided into 2 categories: public-key primarily based} approaches and symmetric-key based approaches .The symmetric-key based mostly approach needs complex key management, lacks of measurability, and isn't resilient to giant numbers of node compromise attacks since the message sender and therefore the receiver have to be compelled to share a secret key. The shared key's employed by the sender to come up with a message authentication code (MAC) for every transmitted message. However, for this methodology, the credibleness and integrity of the message will solely be verified by the node with the shared secret key, that is usually shared by a group of sensing element nodes. Associate degree trespasser will compromise the key by capturing one sensing element node. Additionally, this method doesn't add multicast networks .To solve the measurability drawback, a secret polynomial based message authentication theme was introduced in. the thought of this theme is comparable to a threshold secret sharing, wherever the edge is set by the degree of the polynomial. This approach offers information-theoretic security of the shared secret key once the quantity of messages transmitted is a smaller amount than the edge. The intermediate nodes verify the credibleness of the message through a polynomial analysis. However, once the quantity of messages transmitted is larger than the edge, the polynomial can be absolutely recovered and therefore the system is completely broken.

1.1 Existing System

The public-key primarily based approach, every message is transmitted in conjunction with the digital signature of the message generated mistreatment the sender's personal key. Each intermediate forwarder and also the final receiver will demonstrate the message mistreatment the sender's public key. One amongst the constraints of the public-key primarily based theme is that the high process overhead. Computational complexness, memory usage, and security resilience, since public-key primarily based approaches have a straightforward and clean key management.

1.2 Disadvantages of Existing System

- ✓ High machine and communication overhead.
- ✓ Lack of quantifiability and resilience to node compromise attacks.
- ✓ Polynomial-based theme have the weakness of a intrinsically threshold determined by the degree of the polynomial.

ISSN 2348 – 7968

2. Proposed System

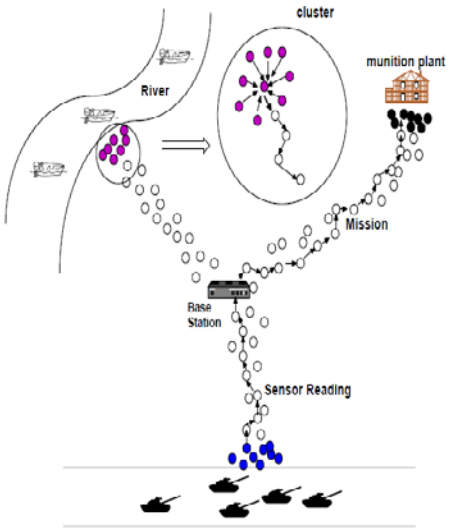
We propose associate categorically secure and economical SAMA. The most plans is that for every message m to be free, the message sender, or the causation node, generates a supply anonymous message critic for the message m. The generation relies on the MES theme on elliptic curves. For a hoop signature, every ring member is needed to reason a forgery signature for all alternative members within the AS. In our theme, the whole SAMA generation needs solely 3 steps that link all non-senders and therefore the message sender to the SAMA alike. Additionally, our style allows the SAMA to be verified through one equation while not severally confirming the signatures.

2.1 Advantages of Proposed System

- A novel and economical SAMA supported computer code. Whereas making certain message sender privacy, SAMA will be applied to any message to produce message content credibleness.
- To provide hop-by-hop message authentication while not the weakness of the built- in threshold of the polynomial-based theme, we tend to then planned a hop-by-hop message authentication theme supported the SAMA.
- When applied to WSNs with mounted sink nodes, we tend to conjointly mentioned potential techniques for compromised node identification.

2.2 System Architecture

Fig 1.Architecture



2.3 Contributions

In this paper, we tend to propose Associate in nursing flatly secure and economical supply anonymous message authentication (SAMA) theme supported the best changed Megamall signature (MES) theme on elliptic curves. This MES theme is secure against adaptative chosen-message attacks within the random oracle model. Our theme allows the intermediate nodes to demonstrate the message in order that all corrupted message is detected and born to conserve the sensing element power. Whereas achieving compromise resiliency, flexible-time authentication and supply identity protection, our theme doesn't have the brink downside. Each theoretical analysis and simulation results demonstrate that our projected theme is a lot of economical than the polynomial-based algorithms below comparable security levels. the most important contributions of this paper are the following:

1. We tend to develop a supply anonymous message authentication code (SAMAC) on elliptic curves that may offer unconditional supply obscurity.
2. We provide Associate in nursing economical hop-by-hop message authentication mechanism for WSNs while not the brink limitation.
3. We tend to devise network implementation criteria on supply node privacy protection in WSNs.
4. We tend to propose Associate in nursing economical key management framework to confirm isolation of the compromised nodes.
5. We offer intensive simulation results below ns-2 and TelosB on multiple security levels. To the simplest of our data, this can be the primary theme that gives hop-by-hop node authentication while not the brink limitation, and has performance higher than the symmetric-key based mostly schemes. The distributed nature of our algorithmic rule makes the theme appropriate for decentralized networks.

2.4 Design Goals

Our projected authentication theme aims at achieving the following goals:

- Message authentication. The message receiver ought to be able to verify whether or not a received message is distributed by the node that's claimed, or by a node in an exceedingly explicit cluster. In alternative words, the adversaries cannot faux to be Associate in nursing innocent node and inject pretend messages into the network while not being detected.
- Message integrity. The message receiver ought to be able to verify whether or not the message has been changed en-route by the adversaries. In alternative words, the adversaries cannot modify the message content while not being detected.
- Hop-by-hop message authentication. Each forwarder on the routing path ought to be able to

ISSN 2348 – 7968

verify the credibleness and integrity of the messages upon reception.

- Identity and site privacy. The adversaries cannot confirm the message sender's ID and site by analyzing the message contents or the native traffic.
- Node compromise resilience. The theme ought to be resilient to node compromise attacks. in spite of what number nodes square measure compromised, the remaining nodes will still be secure.
- Potency. The theme ought to be economical in terms of each machine and communication overhead.

3. Related Work

In [1], [2], even key and hash primarily based authentication schemes were planned for WSNs. In these schemes, every even authentication secret is shared by a group of device nodes. Associate degree trespasser will compromise the key by capturing one device node. Therefore, these schemes aren't resilient to node compromise attacks. Another kind of symmetric-key theme needs synchronization among nodes. These schemes, as well as TESLA [5] and its variants, may also offer message sender authentication. However, this theme needs initial time synchronization, that isn't straightforward to be enforced in giant scale WSNs. additionally, they conjointly introduce delay in message authentication, and therefore the delay will increase because the network scales up.

A secret polynomial based mostly message authentication theme was introduced in [3]. This theme offers info conjectural security with concepts like a threshold secret sharing, wherever the edge is set by the degree of the polynomial. Once the quantity of messages transmitted is below the edge, the theme allows the intermediate node to verify the legitimacy of the message through polynomial analysis. However, once the quantity of messages transmitted is larger than the edge, the polynomial may be absolutely recovered and therefore the system is totally broken. to extend the edge and therefore the complexness for the persona non grata to reconstruct the key polynomial, a random noise, conjointly referred to as a perturbation issue, was additional to the polynomial in [4] to thwart the oppose from computing the constant of the polynomial. However, the additional perturbation issue may be utterly removed victimization error-correcting code techniques [6].

For the public-key based mostly approach, every message is transmitted in conjunction with the digital signature of the message generated victimization the sender's non-public key. Each intermediate forwarder and also the final receiver will evidence the message victimization the sender's public key. The recent progress on ECC shows that the public-key schemes is additional advantageous in terms of memory usage, message quality, and security resilience, since public-key based mostly approaches have a straightforward and clean key management [9].

The existing anonymous communication protocols are for the most part stemmed from either mix net [11] or DC-net [12]. A combine net provides namelessness via packet re-shuffling through a group of mix servers (with a minimum of one being trusted). in a very mix net, a sender encrypts associate degree outgoing message, and therefore the ID of the recipient, exploitation the general public key of the combination. The combination accumulates a batch of encrypted messages, decrypts and reorders these messages, and forwards them to the recipients. Since mix net-like protocols believe the applied math properties of the background traffic, they can't offer obvious namelessness. DC-net [12], [11] is associate degree anonymous multi-party computation theme. Some pairs of the participant's are needed to share secret keys. DC-net provides excellent (information-theoretic) sender namelessness while not requiring trustworthy servers.

However, in DC-net, only 1 user will send at a time, thus it takes extra information measure to handle collision and rivalry.

Recently, message sender namelessness supported ring signatures were introduced. This approach permits the message sender to come up with a supply anonymous message signature with content genuineness assurance. To come up with a hoop signature, a hoop member haphazardly selects associate degree AS and forges a message signature for all alternative members. Then he uses his trap-door data to attach the ring along. The first theme has terribly restricted flexibility and extremely high complexness. Moreover, the first paper solely centered on the cryptographically rule, and also the relevant network problems were left unaddressed.

4. Literature Survey

4.1 Study about Statistical En-route Filtering of Injected False Data in Sensor Networks

In a large-scale device network individual sensors are subject to security compromises. A compromised node will inject into the network giant quantities of fake sensing reports that, if undiscovered, would be forwarded to the information assortment purpose (i.e. the sink). Such attacks by compromised sensors will cause not solely false alarms however conjointly the depletion of the finite quantity of energy in a very battery hopped-up network. During this paper we tend to gift a applied mathematics En-route Filtering (SEF) mechanism which will sight and drop such false reports. SEF needs that every sensing report be valid by multiple keyed message authentication codes (MACs), every generated by a node that detects a

ISSN 2348 – 7968

similar event. Because the report is forwarded, every node on the manner verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink any filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to work out the honesty of every report through collective decision-making by multiple detective work nodes and collective false-report-detection by multiple forwarding nodes. Our analysis and simulations show that, with associate degree overhead of fourteen bytes per report, SEF is in a position to drop 80~90% injected false reports by a compromised node inside ten forwarding hops, and cut back energy consumption by five hundredth or a lot of in several cases.

4.2 Study about an Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks

Sensor networks are typically deployed in unattended environments; therefore exploit these networks at risk of false information injection attacks within which Associate in nursing somebody injects false information into the network with the goal of deceiving the bottom station or depleting the resources of the relaying nodes. Commonplace authentication mechanisms cannot stop this attack if the somebody has compromised one or a little variety of detector nodes. During this paper, we have a tendency to gift Associate in nursing interleaved hop-by-hop authentication theme that guarantees that the bottom station can discover any injected false information packets once no over a particular variety t nodes are compromised. Further, our theme provides Associate in Nursing edge B for the amount of hops that a false information packet can be forwarded before it's detected and born, providing there are up to t colluding compromised nodes. We have a tendency to show that within the worst case B is O (t2). Through performance analysis, we have a tendency to show that our theme is economical with relevancy the protection it provides, and it additionally permits a trade-off between security and performance**.**

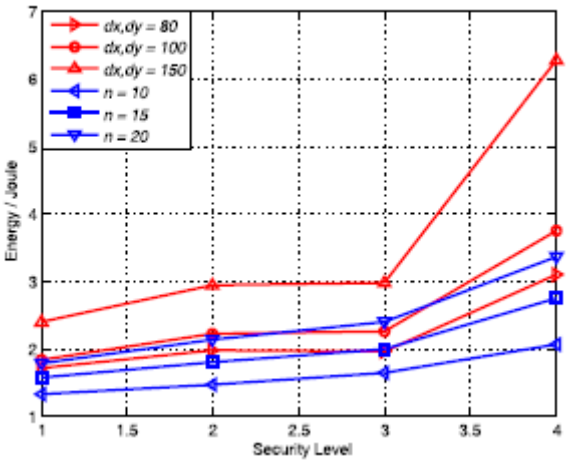
4.3 Study about Lightweight and Compromise-Resilient Message Authentication in Sensor Networks

Numerous authentication schemes are projected within the past for safeguarding communication credibility and integrity in wireless device networks. Most of them but have following limitations: high computation or communication overhead, no resilience to an outsized range of node compromises, delayed authentication, lack of quantifiability, etc. to deal with these problems, we tend to propose during this paper a completely unique message authentication approach that adopts a hot and bothered polynomial-based technique to at the same time accomplish the goals of light-weight, resilience to an outsized range of node compromises, immediate authentication, quantifiability, and non-repudiation. Intensive analysis and experiments have conjointly been conducted to judge the theme in terms of security properties and system overhead.

5 .Simulated Results

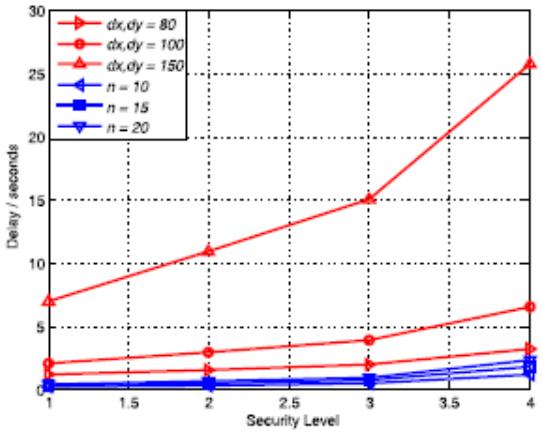
We additionally conduct simulations to match the delivery ratios exploitation ns-2 on RedHat Linux system. The results show that our theme is slightly higher than the quantity polynomial-based theme in delivery quantitative relation. The results square measure given in Fig. 2c.
Our simulation on memory consumption derived in TelosB, sees Table 1, shows the memory consumption for quantity polynomial-based theme is a minimum of 5 times larger than our projected theme.

Fig 2. Performance comparison of our proposed scheme and vicariate polynomial-based scheme

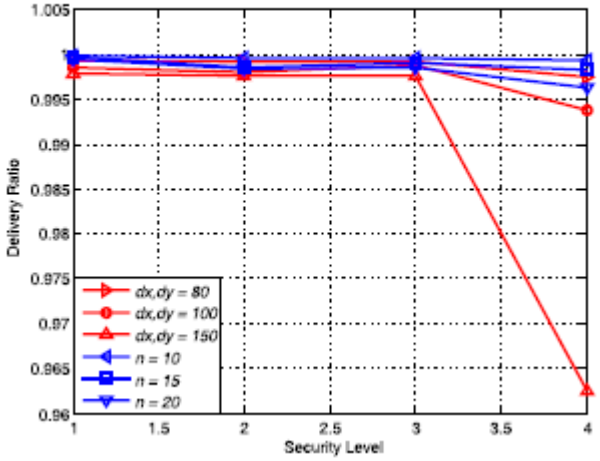


(A).Energy Consumption

ISSN 2348 – 7968



(B).Message Delay



(c).Delivery Ratio

	Polynomial-based approach									Proposed approach									
	$d_x, d_y = 80$			$d_x, d_y = 100$			$d_x, d_y = 150$			$n = 1$			$n = 10$			$n = 15$			$n = 20$		
	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F
$l = 24$	21	3	26	21	4	40	26	4	90	21	1	0	21	2	0	21	2	0	21	2	0
$l = 32$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	2	0
$l = 40$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	3	0
$l = 64$	21	6	64	21	7	100	26	9	225	21	2	0	22	3	0	22	3	0	22	3	0
$l = 80$	21	7	77	21	8	120	26	10	270	20	2	0	21	3	0	21	3	0	21	4	0

Table 1.Memory (KB) for the Two Schemes (TelosB) (F Stands for Flash Memory)

6. Conclusion

In this paper, we tend to 1st planned a unique and economical SAMA supported ECC. Whereas guaranteeing message sender privacy, SAMA will be applied to any message to supply message content genuineness. To supply hop-by-hop message authentication while not the weakness of the built in threshold of the polynomial-based theme, we tend to then planned a hop-by-hop message authentication theme supported the SAMA. Once applied to WSNs with fastened sink nodes, we tend to additionally mentioned attainable techniques for compromised node identification. We tend to compared our planned theme with the quantity polynomial-based theme through simulations victimization ns-2 and TelosB. each theoretical and simulation results show that, in comparable eventualities, our planned theme is a lot of economical than the quantity polynomial-based theme in terms of procedure overhead, energy consumption, delivery quantitative relation, 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,” 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.
[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.

ISSN 2348 – 7968

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

P.Venkata Kiranmai received the B.Tech Degree in Computer Science and Engineering from CVS college of Engineering, University of JNTUA in 2012.She is currently working towards the Master’s Degree in Computer Science and Engineering, in Shree Institute of Technology & Sciences University of JNTUA. She interest lies in the areas of Web Development Platforms, SQL, and Cloud Computing Technology.

M.Sreenivasulu Received M.Tech in Computer Science and Engineering from Sathyabama University. Currently he is an Assistant Professor in the Department of Computer Science and Engineering at Shree Institute of Technology & Sciences-Tirupati.