International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 06, Volume 3 (June 2016) www.ijirae.com

Techniques to Secure Wireless Sensor Networks in Terms of Delay, Process Time and Energy

Divyanshu
Manav Rachna international university

Meenakshi Moza
Manav Rachna international university

Abstract: ***The wireless sensor network system so created and the outcomes so ascertained depend on two standard encryption procedures. In another setting these systems are utilized for security however the exploration paper is assessed on the premise of three distinct parameters in particular delay energy and process time. The most basic piece of this paper is figuring of obligation cycle, which helps in presenting the energy and time delay in both encryption strategies. After broad research and study and computations so done, it has been found that if SAMA strategy is utilized then after effect of delay, energy, and process time all turns out to be better.***

I. INTRODUCTION

Wireless sensor systems (WSNs) comprise of hundreds or even a huge number of little gadgets each with detecting, handling, and correspondence abilities to screen this present reality environment. [1] They are imagined to assume a vital part in a wide assortment of zones going from basic military reconnaissance applications to woodland fire checking and constructing security observing sooner rather than later [2]. In these systems, an expansive number of sensor hubs are conveyed to screen an endless field, where the operational conditions are frequently cruel or even threatening. Be that as it may, the hubs in WSNs have extreme asset imperatives because of their absence of handling force, restricted memory and vitality. [1] Countless hubs are conveyed to screen an unlimited field, where the operational conditions are regularly unforgiving or even antagonistic. In any case, the hubs in WSNs have extreme asset imperatives because of their absence of preparing force, constrained memory. Since these systems are typically conveyed in remote places and left unattended, they ought to be furnished with security instruments to safeguard against assaults, for example, hub catch, physical altering, listening stealthily, disavowal of administration, etc.[3] Unfortunately, customary security components with high overhead are not possible for asset compelled sensor nodes.[4] The analysts in WSN security have proposed different security plans which are improved for these systems with asset limitations. The analysts in WSN security have proposed different security plans which are advanced for these systems with asset imperatives. Various secure and productive steering conventions [5], secure information total conventions and so forth has been proposed by a few analysts in WSN security. [6] Conventional security issues like secure steering and secure information conglomeration, security systems conveyed in WSNs likewise ought to include coordinated efforts among the hubs because of the decentralized way of the systems and nonappearance of any base. [7] Wireless sensor systems comprise of an extensive number of modest smaller scale sensor hubs conveyed in the observing region, which is a multi bounce self-sorting out system framework shaped by remote specialized strategy, whose object is to sense, gather, and process helpfully the data detected by sensors in the system circulated region And then forward the outcomes to its clients. Remote sensor systems, as a rising system advancements, have risen slowly as of late. They are broadly utilized as a part of military safeguard, industry, farming, development and urban administration, biomedical and ecological checking, catastrophe help, open wellbeing and antiterrorism, unsafe and destructive territorial remote control.[8] Wireless system are constrained, which make wireless sensor systems powerless against attack. The security of remote sensor systems is of incredible social concern. Specifically in some essential range, (for example, military target discovery and following), once the sensor system is assaulted or obliterated, this would likely prompt unfortunate results. In this manner, the best approach to plan security instruments can give classification insurance and validation components to forestall vindictive assaults and make a moderately safe workplace for sensor systems, which is a key issue of whether the remote sensor systems are handy. In this manner, the issues and difficulties confronted by remote sensor system security innovation are turning into the fundamental exploration territory everywhere throughout the world.

Message verification assumes a noteworthy part in the unapproved and adulterated messages from being sent in systems to spare the valuable sensor vitality. Hence, numerous validation plans have been proposed in writing to give message validness and uprightness verification for remote sensor systems (WSNs) [9]. These plans can to a great extent be partitioned into two classes: open key based methodologies and symmetric-key based methodologies. The symmetric-key based methodology requires complex key administration, absences of adaptability, and is not strong to huge quantities of hub trade off assaults subsequent to the message sender and the recipient need to share a mystery key. The mutual key is utilized by the sender to produce a message validation code (MAC) for each transmitted message.

Be that as it may, for this technique, the genuineness and respectability of the message must be checked by the hub with the mutual mystery key, which is by and large shared by a gathering of sensor hubs. An interloper can trade off the key by catching a solitary sensor hub. What's more, this strategy does not work in multicast systems.

To take care of the versatility issue, a mystery polynomial based message verification plan was presented in [10]. The possibility of this plan is like a limit mystery sharing, where the edge is dictated by the level of the polynomial. This methodology offers data theoretic security of the mutual mystery key when the quantity of messages transmitted is not exactly the limit. The transitional hubs check the realness of the message through a polynomial assessment. In this paper, we propose an unequivocally secure and productive source unknown message verification (SAMA) plan in view of the ideal changed ElGamal signature (MES) plan on elliptic bends. This MES plan is secure against versatile picked message assaults in the arbitrary prophet model [11]. Wireless sensor network are prone to attacks. There are two types of attacks used in the wireless sensor network namely: hello flood attack and Sybil attack.

Hello flood attack: A few conventions oblige hubs to send HELLO parcels to promote themselves to their neighbors. A hub which gets such a message may expect, to the point that it is inside a radio scope of the sender. It can just re-telecast overhead bundles with enough energy to be gotten by each hub in the network[12] HELLO FLOOD can likewise be considered as one-way, show wormholes. However at times this presumption might be false; some of the time a tablet class aggressor television steering or other data with sufficiently substantial transmission force could persuade each other hub in the system that the assailant is its neighbor.

Sybil attack: In a Sybil attack a hub exhibits different personalities to whatever remains of the hubs. Sybil assaults are a risk to geological steering conventions, since they require the trading of directions for proficient bundle steering. In a perfect world, a hub just sends an arrangement of directions, yet under a Sybil assault, an enemy could put on a show to be in numerous spots at once[13] The Sybil assault can fundamentally lessen the viability of flaw tolerant plans, for example, appropriated capacity, multipath steering, and topology support. Imitations, stockpiling parcels and courses accepted to be utilized by disjoint hubs could as a part of fact be utilized by one single foe exhibiting numerous characters.

The remainder of the paper is organized as follows. Section 2 describes the proposed work. Section 3 presents the methodology part. Section 4 discusses various attacks that can be launched on WSNs. Section 5 presents the result analysis. Finally, Section 6 concludes the paper highlighting some future directions of research in WSN security.

II. PROPOSED WORK

The paper suggests a new parameter in the wireless sensor network for the implementation of the wireless sensor network with various encryption standards to predict the better coup of result as it start with the encryption scheme based on the curve scheme and further technique for the better result part in terms of various parameters.

Polynomial scheme : This scheme show checking message by the polynomial-based scheme i.e. (scheme I) for validating message sent from a reliable base station to normal sensor hubs. Different documentations are to be utilized as a part of the scheme I which are as per the following:

- a, Fa, g, s, γ: a denoted a prime number, Fa is the finite field of order a, g denotes an integer having $2g > a > 2g-1$.
- s, γ: s and γ are to be denoted as integers such that $\gamma < s < l$.

Whereas the scheme-I denoted as the following equation:

$$f(B_1,C_1) = \sum_{0 \le i \le dx\ ,\ 0 \le j \le dy} Di\ ,\ j\ B_g^{\,i} C_g^{\,j}$$

Having the coefficients: Di,j is an element of Fa, and the system parameters dx, dy are the degrees of b and c .

SAMA scheme: Presently the idea of polynomial encryption is considered and its change on elliptic bend ordinarily known as Source Anonymous Message Authentication. The fundamental documentations utilized as a part of SAMA are as per the following:

- m ,a_1 ,a_2 , …… , a_n . Where 'm' is the given message to generate while the set i.e. a_1 , a_2, ….a_n is the public keys of the ambiguity set denoted as:

S = {A_1, A_2 ,…. , A_3} , where the real message sender is A_t, where $1 \le t \le n$, produce the message.
SAMA plan determined the generation and verification of messages.

In generation the first message transmitter and its open key identified with mysterious sender created an unknown message "m" by its private key.

In verification message is to be checked and having S(m) is the unspecified message having people in general key all participators of AS which verify climate the message S(m) which is made by member in equivocalness set.
Taking after condition determines the SAMA scheme:

$$(x_1 , y_1) = cE - \sum_{i=1}^{n} Lihiai$$

$$= (K_t + \sum_{i \neq t} Ki + L_t d_t h_t) E - \sum_{i} Lihiai$$

$$= \sum_{i \neq t} kiE + (k_t E - \sum_{i \neq t} Lihiai)$$

$$= \sum_{i \neq t} (Li, Mi) + (L_t , M_t)$$

$$= \sum_{i} (Li, Mi)$$

III. METHODOLOGY

The plan particular for the working of polynomial is as in taking after strides:
***Introduction of Sensor Nodes*:** Before a sensor hub is conveyed, it is preloaded by the security server with:

- A one of a kind ID n, which is a component of Fa
- Polynomial verfu(y)=f(n,y), which is known as the confirmation polynomial of hub n.
- The secure one-way hash capacity h(.).

***Message Sending at the Base Station*:** Assuming the base station needs to convey a message, meant as m, it executes the accompanying strides to sign m:
- Hash capacity h(.) is connected on m to get h(m).
- Polynomial f(x,y) is assessed at y = h(m) to get a univariate dx-degree polynomial MAFm(x)= f(x,h(m)), which is known as the message validation capacity for m.
- Message m,MAFm(x) is conveyed, where MAFm(x) is spoken to by its dx+1coefficients.

***Message confirmation at Sensor Nodes*:** When a sensor hub with ID n gets message m,MAFm(x), it executes the accompanying strides to check the credibility and trustworthiness of the message:
- h(.) is connected on m to get h(m).
- verfu(y) is assessed at y = h(m) to get verfv(n,h(m)).
- Received MAFm(x) is assessed at x = u to get MAFm(n).
- If and just if verfv(n,h(m)) = MAFm(v),they got message is viewed as genuine and in place.

The plan detail for the working of SAMA is as in taking after strides:
A SAMA comprises of the accompanying two calculations:
- Generate (m;a1;a2;...;an). Given a message m and the general population keys a1;a2;...;an of the AS. S={A1,A2,...,An}, the genuine message sender At, produces an unknown message S(m) utilizing its own particular private key dt.
- Verify S(m). Given a message m and an unknown message S(m), which incorporates people in general keys of all individuals in the AS, a verifier can figure out if S(m) is created by a part in the AS.

For the Generation calculation, suppose ‘m’ is a message to be transmitted. The private key of the message sender Alice is dt. To produce an effective SAMA for message m, Alice performs the accompanying strides:

1. Select an arbitrary and pairwise distinctive ki for each1≤ i ≤n-1; i≠ t and process ri from (ri,yi)= kiE.
2. Pick an arbitrary ki € Zp and register rt from (rt,yt)=ktE-Σ ri hello there Qi such that rt=0 and rt≠ ri for any i≠t and the SAMA of the message m is defined as:

S(m)=(m,S,r1,y1,...,rn,yn,s).

IV. ATTACKS:

Attacks on layers: Different layers connecting by one another by the use of protocols delivers the response of the system. By this research paper propose that various attacks techniques can distress in various possible layers namely: physical, data – link, network and Transport layer. The layer known as physical layer is the main layer which offers the discreet to the layer by offer physical connection these attack in this layer can make the system poor in case of the response rate . The base of the Sybil attack is really physical layer yet it turns out to be more incite in the higher layers like connection layer and system layer. In this class of assault, the enemy brings a vindictive hub into the network.[14] This malevolent hub get characters by two courses: by manufacturing or by taking. The pernicious hub acts as though it were of various personalities of better places in the system.

In hello flood attack WSN oblige hubs to show hello messages to declare themselves to their neighbors. A hub which gets such a message may accept, to the point that it is inside a radio scope of the sender.[12]. Be that as it may, those hubs which are adequately far from the enemy would send the bundles into obscurity. Consequently the system is left in a mess. Conventions which rely on upon confined data trade between neighboring hubs for topology upkeep or stream control are principally influenced by this sort of attack.

In this Data –link layer a foe can impel impact in one and only little parcel of the whole bundle transmitted by a hub. A little change in the information segment of the parcel prompts a mistake in the checksum of the entire bundle and requests retransmission of the same bundle.

Sybil attack is particularly noticeable in the Link Layer. Distinctive varieties of Sybil Attacks are as per the following:

***DATA Aggregation*:** DATA collection is a vital part in Wireless Sensor Networks as it diminishes the force utilization and in addition the data transfer capacity necessities for individual message transmission.[14] In this circumstance, a Sybil Attack can be utilized to incite negative fortifications. A solitary malevolent hub is adequate to go about as various Sybil Nodes and afterward this may give numerous negative fortifications to make the total message a false one.

***Voting*:** Voting might be a decision for various errands in a Wireless Sensor Network. Numerous MAC conventions may go for voting in favor of finding the better connection for transmission from a pool of accessible connections. Here, the Sybil Attack could be utilized to stuff the tallying station. An assailant might have the capacity to decide the result of any voting and, obviously, it relies on upon the quantities of characters the aggressor claims.

Numerous conventions oblige hubs to telecast HELLO packets to report themselves to their neighbors if a hub gets such parcel, it would expect that it is inside the RF scope of the hub that sent that bundle. Not with standing, this suspicion could be false on the grounds that a portable PC class foe could without much of a stretch send these bundles with enough energy to persuade all the system hubs that the enemy is their neighbor. Yet, the transmission force of those hubs is considerably less that the adversary's, in this manner the bundles would get lost, and that would make a mess in the sensor system [13].

In the system layer each qualified recipient ought to get all messages planned for it. Each getting hub ought to likewise have the capacity to check the honesty of each message and additionally the personality of the sensor.[14] The Routing convention ought to likewise be in charge of forestalling listening stealthily brought about by abuse or manhandle of the convention itself. All multi-way directing conventions are helpless against Sybil attack. The vindictive hub present in the system may publicize diverse personalities. At that point all ways in the multipath convention may go through the malevolent hub. What's more, the convention may have a photo of presence of various ways. In any case it is the same way through the noxious hub. Sybil attack can really trick the convention giving a photo of presence of various directing ways to the destination however it is the same way through the Sybil node.[14] On top of that even Geographic Routing Protocols are helpless against Sybil attack. It is a result of the way that the same Sybil Identity or diverse Sybil Nodes may give a fantasy of their nearness at various geographic areas.

Hello flood attack is an attack on the system layer , numerous steering conventions oblige hubs to show Hello parcels to declare themselves to their neighbors, and a hub accepting such a bundle may expect, to the point that it is inside typical radio scope of the sender.[13] This suspicion may in some cases are false; a portable workstation class assailant television directing or other data with sufficiently substantial transmission force could persuade each hub in the system that the enemy is it neighbors. A hub understanding the connection to the enemy, which is false, could be left with couple of choices: all its neighbors may endeavor to forward bundles to the foe too. Conventions which rely on upon confined data trade between neighboring hubs for topology upkeep or stream control are likewise subject to this attack.

For make the association with be secured and to port the information bits and its different bits to application and the presentation layer, the transportation layer is particularly capable. The Sybil and hello flood attack on this layer influences the execution as they have a tendency to decrease the execution.

A Sybil node is a getting out of hand hub's extra character. In this way, a solitary element might be chosen various times in view of different personalities to take part in an operation that depends on excess, in this manner controlling the result of the operation and vanquishing the repetition instruments.

Numerous conventions which utilize HELLO bundles make the gullible supposition that accepting such a parcel means the sender is inside radio range and is accordingly a neighbor. A foe may utilize a powerful transmitter to trap a huge region of hubs into trusting they are neighbors of that transmitting hub [13]. In the event that the foe dishonestly shows a better course than the base station, these hubs will endeavor transmission to the assaulting hub, regardless of numerous being out of radio reach in all actuality.

V. RESULT ANALYSIS

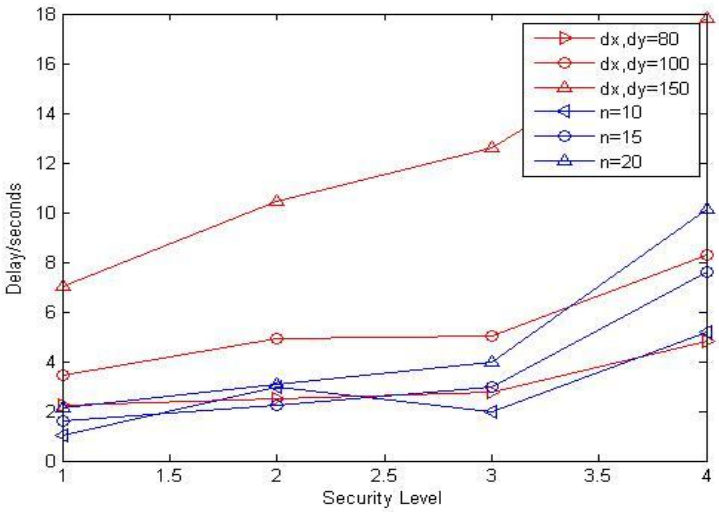

Figure 1.1: Message delay

By comparing the two encryption technique on basis of their message delay in polynomial technique the message delay if much more than in the SAMA technique which means as the no. of users increases for the higher degree polynomial the message delay will be more as compare with SAMA

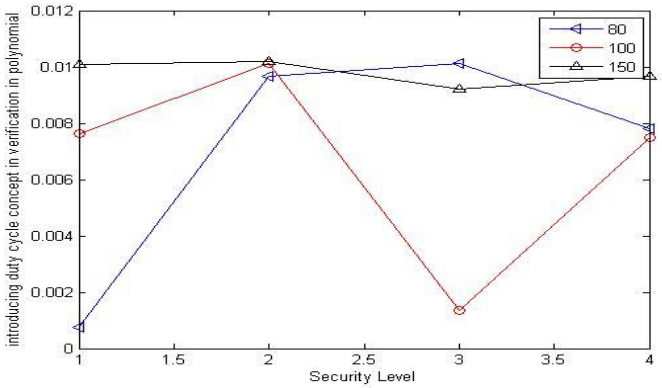

Figure 1.2: Concept of duty cycle in verification of polynomial

As the no. of user's increases or the no. of the security level increases, the duty cycle also increases with the no. of user's or security levels which means that it consumes more time and more energy for the verification.

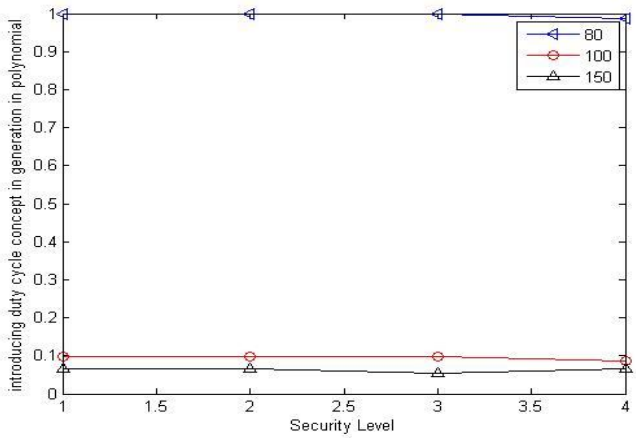

FIGURE 1.3: Concept of duty cycle in generation of polynomial

In generation of the polynomial technique, the energy and the time taken with security levels the duty cycle is found to be lower as compared with the verification.

	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	
	Gen	Verify	Gen	Verify	Gen	Verify	Gen	verify	Gen	verify	Gen	Verify	Gen	Verify
l=24	6.6493	0.0002	12.7202	0.0002	26.3383	0.0002	0.2248	0.5004	4.1746	2.3769	6.3449	3.4399	8.5439	4.4723
l=32	9.4579	0.0002	18.6351	0.0002	39.3589	0.0002	0.3294	0.7047	5.9870	3.3146	8.9231	5.0181	12.1908	6.8614
l=40	10.4876	0.0002	19.2392	0.0002	40.4473	0.0002	0.4551	1.0329	7.8931	4.4240	11.7977	6.6747	16.2041	8.9001
l=64	18.6329	0.0002	31.7260	0.0002	68.5826	0.0002	1.1757	1.7048	20.6285	11.3779	30.2984	16.8315	40.5027	22.2545
l=80	23.5704	0.0002	38.8238	0.0002	84.9328	0.0002	1.4103	2.1895	26.3457	13.8779	37.5184	20.8183	50.7265	25.7772

Table 1.1: Process time comparison table

Polynomial Scheme and proposed `scheme comparison with respect to generation and verification time taken in the process for different values of L=24, 32, 40 64, 80.For polynomial-based scheme, the time for generation procedure is especially shorter than the verifying time; in the interim, for our proposed plan, the verification time is much shorter than the validation generation time. Our scheme is more productive for hop by-hop validation under comparable security levels. All the more essentially, the verification time for our scheme is much shorter than the bivariate polynomial-based scheme's since confirmation will be led in various multiple hops.

VI. CONCLUSION

The main aim of the paper is to generate a scenario of WSN which is based on the two different encryption schemes. If a network having the user node as its part then that user node will attempt to acknowledge as an authentic node. If it passes through the encryption scheme having the security then only the result will verified of the node. But if node is use then it communicates with number of nodes present at base station and other nodes, the generation as well as the verification process results in enhancement of secure network. To evaluate the execution of two procedures of generation and verification of the polynomial scheme and SAMA is computed and afterward the outcomes are discovered then the estimations of results utilizing a novel parameter duty cycle has demonstrated that SAMA is superior to anything polynomial in all circles.

REFRENCES

[1]. Jaydip Sen ″A Survey on Wireless Sensor Network Security″ International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009.
[2]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine, Vol.40, No. 8, pp. 102-114, August 2002.
[3]. S. Ganeriwal and M. Srivastava, “Reputation-based framework for high integrity sensor networks”, In Proceedings of the 2nd ACM Workshop on Security on Ad Hoc and Sensor Networks, Washington DC, USA, 2004.
[4]. B. Karp and H.T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks”, In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 243-254, ACM Press, 2000.
[5]. P. Papadimitratos and Z.J. Haas, “Secure routing for mobile ad hoc networks”, In Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002) 2002.
[6]. D. Estrin, R. Govindan, J.S. Heidemann, and S. Kumar, “Next century challenges: Scalable coordination in sensor networks”, Mobile Computing and Networking, pp. 263-270, 1999.
[7]. L. Hu and D. Evans, “Secure aggregation for wireless networks”, In Proceedings of the Symposium on Applications and the Internet Workshops, 2003, pp. 384, IEEE Computer Society, 2003.
[8]. Qiuwei Yang, Xiaogang Zhu, Hongjuan Fu, and Xiqiang Che Survey of Security Technologies on Wireless Sensor Network″ Hindawi Publishing Corporation Journal of Sensors Volume 2015, Article ID 842392.
[9]. Jian Li, Yun Li, Jian Ren, and Jie Wu ″Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks″ IEEE transactions on parallel and distributed systems, vol. 25, no. 5, may 2014.
[10]. 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.
[11]. Wensheng Zhang , Nalin Subramanian and Guiling Wang ″Lightweight and Compromise-Resilient Message Authentication in Sensor Networks″ IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings.
[12]. Virendra Pal Singh , Sweta Jain and Jyoti Singhai ″Hello Flood Attack and its Countermeasures in Wireless Sensor Networks″ IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.
[13]. Shikha Magotra and Krishan Kumar ″ Detection of HELLO flood Attack on LEACH Protocol″ 2014 IEEE International Advance Computing Conference.
[14]. Hiren Kumar Deva Sarma Avijit Kar ″Security Threats in Wireless Sensor Networks″ IEEE A&E systems magazine, june 2008.

