IJCSET – Volume 7, Issue 6 JUNE 2021. ISSN: 2455-9091 Pages: 13-21

International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)- NEW DELHI INDIA .
ISSN :2455-9091

A SURVEY ON IMPLEMENTATION SOLUTIONS FOR ATTACK PREVENTION CRYPTOGRAPHY TECHNIQUES IN WSN USING NS2

[1] G. BANUPRIYA, [2] DR. P. LOGESWARI
[1] Research Scholar, [2] Assistant Professor,
[2] Department of Computer Science,
[1, 2] Sri Krishna Arts & Science College,
[1, 2] Coimbatore, Tamilnadu, India.

ABSTRACT - Because of absence of alters safe equipment and broadcast nature of Wireless Sensor Networks (WSNs), security in sensor networks is one of the significant concerns. In this paper we survey on implementation solutions for attack prevention different cryptography techniques. WSNs comprise of countless sensor nodes and a couple of sink nodes or Storage node is utilized to gather data about the condition of actual world and communicate it to intrigued clients. It utilized in applications, for example, wellbeing checking, natural surroundings observing, military reconnaissance and climate detecting. Sensor nodes have restricted assets in term of handling power, battery force, and information stockpiling. A sensor network that isn't completely believed that is the reason protection is to be safeguarded. A security approaches that utilization secret key cryptography and key administration. To safeguard the trustworthiness, a computerized key is gotten to each node in an organization, every node needs to send their confinement position as scrambled information utilizing advanced marks to the capacity node and it decodes that information and checks the situation by utilizing verification.

Keywords: [Wireless Sensor Networks; Cryptography; Attack Prevention; sensor network.]

1. INTRODUCTION

Wireless sensor networks have arises as cutting edge innovation in data innovation environment and exploration including equipment framework plan, information the executives, security and social factors. Sensor networks allude to a heterogeneous framework joining little sensors and actuators with universally useful processing components. Sensor node is a keen, little, self getting sorted out, low cast, and multi-practical gadget, outfitted with battery, radio correspondence, microcontroller and sensor. It has extremely restricted handling capacity battery force, memory and furthermore a limited field of detecting. The primary reason for WSN is to fill in as an interface to genuine world, giving actual data like temperature, light, radiation and so forth to a PC framework. In this paper to address the basic security issues in WSNs we examine about cryptography. Sensor networks allude to a heterogeneous framework joining small sensors and actuators with universally useful figuring components. These networks will comprise of hundreds or thousands of self-coordinating, low force, ease wireless nodes conveyed to screen and influence the climate. Sensor networks are regularly portrayed by restricted force supplies, low transfer speed, little memory sizes and restricted energy. This prompts a requesting climate to give security. Classification is concealing the data from unapproved access. In numerous applications, nodes impart exceptionally delicate information. A sensor organization ought not to break sensor perusing to adjoining networks. Simple strategy to maintain delicate information mystery is to scramble the information with a mysterious key that solitary the expected receivers 'possess, henceforth accomplishing confidentiality. As public key cryptography is too costly to ever be American Journal of Engineering utilized in the asset obliged sensor networks, most of the proposed conventions utilize symmetric key encryption methods. For symmetric key methodology the key conveyance component ought to be incredibly powerful. Validation guarantees the unwavering quality of the message by recognizing its origin.

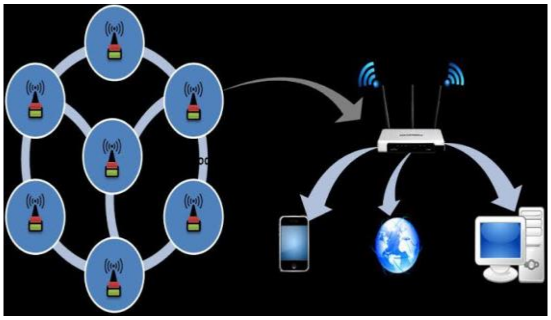

Figure 1.Wireless sensor networks using NS2

In a WSN, the issue of confirmation should address the accompanying prerequisites: imparting node is the one that it professes to be the recipient ought to check that they got parcels have evidently come from the genuine sensor node. For Authentication to be accomplished the two gatherings should share a mysterious key to process Message verification code (MAC) of all conveyed data. The collector will check the validation of the got message by utilizing the MAC key. Uprightness is keeping the data from unapproved modification. Data validation can give information respectability too. Accessibility guarantees that administrations and data can be gotten to at the time they are required. In sensor networks there are numerous dangers that could bring about loss of accessibility, for example, sensor node catching and disavowal of administration assaults. Probably the greatest test with regards to getting MANETs and WSNs is the entirety of the elements that should be represented: unique geographies, asset requirements, no foundation and restricted actual security. As WSNs ordinarily have a greater number of nodes than MANETs, and sensory nodes in WSNs are more assets compelled regarding power, computational capacities, and memory, the security configuration utilized in WSNs must be more explicit for those spaces. Much exploration has been led on directing security, key administration, and trust in MANETs and WSNs; a large portion of it is related with cryptography, validation, approval, encryption, and unscrambling. The definite cycle can be found through different reviews and advancement of cryptography instruments for MANETs/WSNs.

2. LITERATURE SURVEY

1. A. A. Adekunle (2015), et.al proposed A Symmetric Cryptographic Construct for Securing Wireless Sensor Network Communications. AEAD schemes can be delegated possibly one-pass or two pass schemes. In a two-pass plot, the arrangement of secrecy and uprightness security administrations is given in isolated passes. A strategy for building two-pass AEAD schemes is by conventional synthesis; whereby one-pass is a security just symmetric encryption conspire, while the other pass is a message trustworthiness plot. In a one-pass plot, a solitary pass is made through the information, which all the while produces secrecy and trustworthiness security to the handled information. Typically, one-pass schemes for the most part display higher information handling rate and lower operational expenses.

Merits

Cypher Codex build exhibited favorable execution with respect to a high information handling throughput, low preparing inactivity and a demonstrated low energy use prerequisite across a scope of reasonable WSN conveyed bundle lengths.

Demerits:

Prior to any correspondence, both the sender and the receiver need to concede to a mystery symmetric key. It requires a protected key foundation instrument set up.

2. Constantin Grumazescu, Valentin-Alexandru Vladuta,Andrei Timofte(2018), et.al proposed Hybrid identity based cryptographic scheme optimization using machine learning in WSN to revamp the security foundation to advance force utilization of sensor nodes dependent on qualities gathered by a UAV at every cycle the best up-and-comer calculation we are thinking about here is K-implies. At first considering an irregular or client characterized number of k PKG nodes out of n absolute nodes (with k < n) an orchestrator occurrence can figure the centroids of the security foundation to equitably circulate the force utilization level of sensor nodes. The distance capacity can be viewed as the Euclidean distance between the utilization levels of every sensor node. This information can be accumulated in an old style way by utilizing at least one static sinks or a mobile sink (UAV), totaled, deciphered, prepared and the outcomes directed a similar way.

Merits:

Client prerequisites for both organization life expectancy and security level are accomplished.

Demerits:

This must be finished utilizing AI procedures.

3. Jyothi Metan, K N Narasimha Murthy(2015), et.al proposed Robust and Secure Key Management in WSN using Arbitrary Key-Deployment the space of wireless sensor network is as of now covered with different issues for example energy issues, steering issues, QoS issues, and security issues. Albeit in past there were development of different secure procedures, however dominant part of the method were refined cryptographic executions where reality intricacies were less accentuated. This paper presents a basic and a novel procedure called as MLKS for example Staggered Key Security that applies straightforward set hypothesis and key dissemination tool for getting the data in wireless sensor network. The strategy is likewise material on various security principles supporting 128, 216, 160, or 512 pieces of key size. The result of the proposed framework is contrasted with the main work with discover the proposed framework outflanks the current framework as for computational time and capacity cost.

Merits

This procedure that tends to various degrees of safety tasks for together tending to security in bunch correspondence just as information conglomeration in wireless sensor network.

Demerits

Nonattendance of novel digital signature plan to make the current gathering correspondence safer.

4. Trong-Minh Hoang,Van-Hau Bui,Nhu-Lan Vu(2020), et.al proposed A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks. Wireless Sensor Network (WSN) is a significant part of the Internet of Things design. It works in antagonistic climate areas to give a ton of intriguing applications. Nonetheless, WSN is compelled by restricted assets like force or computational expense, making it helpless against numerous sorts of assaults. Henceforth, tracking down a fitting security answer for ensure node validation and sensor information respectability which are two of the most basic security issues has consistently pulled in scientists. In which, the digital watermarking strategy can be utilized to get sensory information while keeping a sensible calculation cost. In any case, these days, node clone assaults can make a conflict of inside assaults which harms vigorously to the exhibition of sensor networks. Henceforth, the classification and trustworthiness of sensor network elements are raised more provokes identified with intricacy and viable issues. This paper proposes a novel lightweight blended secure plan dependent on watermarking strategies to ensure sensory information and guard against node clone assaults. Mathematical outcomes and security examination will be given in the paper to approve the benefit of the proposed security convention.

Merits

A center convention related to an execution algorithm to shield the sensor network node from node parodying assaults while ensuring the information gathered by the sensor network.

Demerits

WSNs network when identifying an assault with both private and worldwide algorithms isn't reacting.

5. Tarek Farah, Safya Belghith (2017), et.al proposed A new chaotic encryption algorithm for WSN and implementation with sensors AS-XM1000. The degree of safety changes starting with one area then onto the next and starting with one application then onto the next relying upon the kind and significance of the information traded in the remote sensors. In this paper we propose to imagine a chaotic encryption algorithm for WSN dependent on S-box and chaotic stages. Correlations other proposed algorithms are introduced in this paper. The aftereffects of the assessments and estimations of the proposed algorithm tests are finished by utilizing the TinyOS working framework, which makes it conceivable to deal with the assets of the WSN. We will likewise introduce an execution of the proposed algorithm on AS-XM1000 sensors. The proposed technique is adaptable; surely the proposed encryption algorithm can be applied to messages of little size or enormous size as on account of pictures

Merits

Encryption technique can monitor the information and correspondence from unapproved disclosure and access of information.

Demerits

The organization or the PC framework can be assaulted and delivered non-useful by a gatecrasher.

6. Pritam Banerjee, Tanusree Chatterjee, Sipra DasBit (2015), et.al proposed Low-overhead Encryption based Node Authentication in WSN. Execution of the plan is basically broke down by utilizing two appropriately picked boundaries like breaking likelihood and breaking time. This assessment guides us in fixing the size of the exceptional id of a node so the plan brings about low overhead just as accomplishes adequate power. The presentation is additionally contrasted a few late works as far as calculation and correspondence overheads and that affirms our plan's matchless quality over contending plans as far as both the measurements.

Merits:

This is light weighted by utilizing computationally light activities like Ex-OR, extraction, bitwise mix.

Demerits:

There is no coordinating message validation with the node verification to make a more complete security answer for WSNs.

7. Chungen Xu, Yanhong Ge(2009), et.al proposed The Public Key Encryption to Improve the Security on Wireless Sensor Networks. Wireless sensor networks (WSN) develops and gains new in our lives. Anyway security in WSN was not painstakingly completed, since just some symmetric encryption based conventions are proposed in writing, under the supposition that the idea of sensor nodes doesn't uphold public key encryption because of the constraint in battery and CPU power. This paper presents a plan of Public Key Infrastructure (PKI) for wireless sensor networks. The plan attempts to take care of the issue of safety in WSN by the utilization of public key cryptography as an instrument for guaranteeing the legitimacy of the base station, and propose a RSA's execution of Public Key Encryption to improve the security on wireless sensor networks.

Merits

The plan attempts to tackle the issue of safety in WSN by the utilization of public key cryptography as an apparatus for guaranteeing the validness of the base station.

Demerits

One hindrance of public-key encryption is that is slower than different techniques, like mystery key encryption. In secret-key encryption, a solitary key gives that best way to encode and decode, improving and accelerating the interaction.

8. Zhang Jing, Ma Chen, Fan Hongbo (2017), et.al proposed WSN Key Management Scheme Based on Fully Bomomorphic Encryption. Improving the safe WSN's continuous, energy utilization, and against spill is a significant exploration issue in view of explicit activities as expansion, duplication, etc. Completely homomorphic encryption can control the cipher text straightforwardly to get the right outcomes without unscrambling. Since completely homomorphic encryption's interaction of the unscrambling can be precluded, the safe WSN's qualities, for example, continuous, etc can be improved adequately. Key administration is a significant issue of completely homomorphic encryption, in which the capacity to hostile to catch in WSN starts things out. In this paper, in light of the estimation calculation of two component even polynomials proposed by Blundo, we propose a pair wise key foundation plot by presenting completely homomorphic encryption, which doesn't just forestall adversary catching data about polynomial connection, yet in addition oppose the huge scope node catch assault effectively. Examination and tests show that this plan can absolutely meet the prerequisites of asset, energy utilization, etc of WSN, and improve the security of WSN at the same time.

Merits

The energy utilization of the nodes has an excellent improvement.

Demerits

The homomorphic encryption requires either application changes or devoted and concentrated customer worker applications to make it work practically.

9. Yan Liu, Xiumei Wu, Xuemin Chen (2015), et.al proposed A Scheme for Key Distribution in Wireless Sensor Network Based on Hierarchical Identity-Based Encryption. Customary technique for key appropriation doesn't fit the need to run in wireless sensor organization (WSN) because of limit on energy, calculation and memory limit of WSN. In this paper, we propose a plan based on Hierarchical Identity Based Encryption (HIBE) to convey encode key. Contrasting and key appropriation based on

Identity-Based Encryption (IBE), the proposed conspire lessens the calculation time and saves memory space of wireless sensor node.

Merits

Wireless sensor networks by embracing the HIBE to save the extra room and to decrease the calculation needed at every node.

Demerits

This requires a more significant level of affirmation and accessibility from PKG side. This is disadvantage of IBE System.

10. Shao-I Chu, Yu-Jung Huang, Wei-Cheng Lin (2015), et.al proposed Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for Wireless Sensor Networks. Wireless sensor networks (WSNs) have been broadly utilized, most outstandingly continuously traffic checking and military detecting and following. Be that as it may, WSN applications could experience the ill effects of dangers and imperil the applications if the reasonable security issues are not mulled over. Subsequently, client confirmation is a significant worry to shield information access from unapproved clients. Rather than generally utilizing a hash work for information security, one of the fascinating parts of this convention is that, with the end goal of information assurance however with a low computational expense, the proposed key encryption work just requires straightforward selective OR (XOR) number-crunching tasks. In addition, the relating equipment design was carried out by utilizing an Altera DE2 board, including an Altera Cyclone II field-programmable gate array (FPGA). At last, the yield waveforms from the FPGA were shown on the 16702A rationale investigation framework for constant check.

Merits

A lightweight common confirmation convention over WSNs is produced for secure validation.

Demerits:

This isn't reasonable for encryption of huge messages as the encryption/decoding throughput is contrarily identified with the key length.

11. A. Karthikeyan, V. Srividhya, Pranjay Gupta, Naveen Rai,(2015), et.al proposed a Discrete cosine and Discrete Wavelet transform based algorithm for simultaneous image compression and encryption is proposed, which is useful for reliable data transmission. The Secure Force encryption algorithm utilized is appropriate to wireless sensor networks (WSN). The adequacy of our proposed algorithm is assessed based on the PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), registering time and rate pressure. The proposed algorithm helps in diminishing information repetition altogether which makes it energy proficient while thinking of it as' usage for WSN.

Merits:

An energy effective concurrent pressure and encryption algorithm explicitly for wireless sensor networks to be utilized for military or energy driven applications.
This will reduce the encrypting complexity.

Demerits:

This will decrease the scrambling intricacy.

12. Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef (2012), et.al proposed Performance Evaluation of Encryption Algorithm for Wireless Sensor Networks. With the far reaching development in applications for asset restricted Wireless Sensor Networks (WSN), the requirement for dependable and effective security systems for them has expanded complex yet its execution is a non-minor assignment. Impediments in preparing speed, battery force, transmission capacity and memory oblige the materialness of existing cryptography Algorithms for WSNs. A few security systems, like TinySec, have been acquainted with address the requirement for security in WSNs. The expense of safety, be that as it may, in any case generally stays an obscure variable. To give a superior comprehension of this expense we have considered three encryption algorithms, AES, RC5 and RC6. We have estimated and looked at their memory and energy utilization on Mica2 sensor bits.

Merits

Cryptographic algorithms are crucial for the protected and proficient improvement of cryptosystem in gadgets with low computational force.

Demerits

Versatile cryptographic components to streamline energy utilization by shifting code boundaries with convenient procurement of asset setting in WSN climate can't be investigated.

13. Jia Chenjun, Liao Yongjian, Chen Kangshen(2008), et.al proposed Secure Encryption in Wireless Sensor Network. Wireless sensor networks (WSN) have gotten a great deal of consideration as of late because of their wide scope of uses in military just as regular citizen activities. It is a moving work to plan reasonable cryptography for wireless sensor networks since the impediments of force, calculation ability, and capacity assets. Numerous plans dependent on symmetric or public key cryptography have been examined. As of late, a reasonable personality based encryption method is proposed.

Merits

Effective personality based encryption plot which has been demonstrated secure in the wireless sensor network climate while decreases the necessity of asset.

Demerits

In the event that you use encryption to secure your data on your PC at work or at home, it could raise doubts.

14. Xueying Zhang, Howard M. Heys, and Cheng Li (2010), et.al proposed An Analysis of Link Layer Encryption Schemes in Wireless Sensor Networks. In particular, we research various variables which influence the energy cost of link layer cryptographic security schemes, for example, the payload size, the wellspring of the introduction vector, and the channel quality. We propose a way to deal with assess the exhibition of cryptographic correspondence schemes by building up an examination model thinking about these components. The propriety of this model is upheld by reenactment results.

Merits:

The cipher criticism conspire accomplishes better execution for a scope of channel characteristics and for little payload sizes gives a huge relative improvement in the quantity of the pieces that can be effectively moved for a given energy.

Demerits

Key circulation and the board are more mind boggling in light of the fact that each bounce gadget should get a key, and when the keys change, each should be refreshed.

15. Mustafa A. Al Sibahee, Songfeng LU (2017), et.al proposed The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN. Wireless Sensor Networks (WSNs), applications are developing quickly, so the necessities to ensure such applications are expanded. Cryptography assumes a principle part in data framework security where encryption calculation is the fundamental segment of the security. On the opposite side, those calculations burn-through a lot of figuring assets, for example, CPU time, memory, and battery power.

Merits

Encryption is utilized to secure delicate information, including individual data for people.

Demerits:

Utilizing encrypted documents that are intended to be opened and shared by at least two individuals can be disadvantageous when at least one member thinks that it's a weight to utilize encryption.

CONCLUSION

Wireless multimedia sensor networks will assume a significant part in the Internet of Things world, since current observing applications will depend on multimedia information for more hearty choices. In this specific circumstance, cryptography will be in WMSN plan. In this paper we surveyed existing cryptography techniques for attack prevention. Late works have proposed many promising answers for give various degrees of safety in those organization, which will impact the manner in which security will be given in current WMSNs. The issue of adding nodes to a current organization is troublesome, even with public key cryptography, as each node in this disseminated network must be educated about recently added and acknowledged public keys. Repudiation is considerably harder, in light of a few entanglements.

REFERENCES

[1]. A. A. Adekunle, "A symmetric cryptographic construct for securing wireless sensor network communications," 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), 2015, pp. 935-940, doi: 10.1109/IWCMC.2015.7289208.

[2]. C. Grumazescu, V. Vladuta and A. Timofte, "Hybrid identity based cryptographic scheme optimization using machine learning in WSN," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2018, pp. 1-6, doi: 10.1109/ECAI.2018.8678972.

[3]. J. Metan and K. N. Narasimha Murthy, "Robust and secure key management in WSN using arbitrary key-deployment," 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), 2015, pp. 246-250, doi: 10.1109/ERECT.2015.7499021.

[4]. T. Hoang, V. Bui, N. Vu and D. Hoang, "A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks," 2020 International Conference on Information Networking (ICOIN), 2020, pp. 649-653, doi: 10.1109/ICOIN48656.2020.9016541.

[5]. T. Farah and S. Belghith, "A new chaotic encryption algorithm for WSN and implementation with sensors AS-XM1000," 2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2017, pp. 684-689, doi: 10.1109/STA.2017.8314968.

[6]. P. Banerjee, T. Chatterjee and S. DasBit, "LoENA: Low-overhead encryption based node authentication in WSN," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 2126-2132, doi: 10.1109/ICACCI.2015.7275931.

[7]. Z. Jing, M. Chen and F. Hongbo, "WSN key management scheme based on fully bomomorphic encryption," 2017 29th Chinese Control And Decision Conference (CCDC), 2017, pp. 7304-7309, doi: 10.1109/CCDC.2017.7978504.

[8]. R. Weper, E. Zehendner and W. Erhard, "/spl rho/: hierarchical modeling of parallel architectures," Proceedings of the Seventh Euromicro Workshop on Parallel and Distributed Processing. PDP'99, 1999, pp. 233-240, doi: 10.1109/EMPDP.1999.746678.

[9]. S. Chu, Y. Huang and W. Lin, "Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for Wireless Sensor Networks," in IEEE Systems Journal, vol. 11,

no. 4, pp. 2718-2725, Dec. 2017, doi: 10.1109/JSYST.2015.2487508.

[10]. A. Karthikeyan, V. Srividhya, P. Gupta and N. Rai, "A novel approach for simultaneous compression and encryption of image in wireless media sensor network," 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2015, pp. 364-369, doi: 10.1109/ICATCCT.2015.7456911.

[11]. M. A. Al Sibahee, S. Lu, Z. A. Hussien, M. A. Hussain, K. A. Mutlaq and Z. A. Abduljabbar, "The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN," 2017 International Conference on Computing Intelligence and Information System (CIIS), 2017, pp. 308-312, doi: 10.1109/CIIS.2017.50.

[12]. X. Zhang, H. M. Heys and C. Li, "An Analysis of Link Layer Encryption Schemes in Wireless Sensor Networks," 2010 IEEE International Conference on Communications, 2010, pp. 1-6, doi: 10.1109/ICC.2010.5502145.

[13]. N. Bandirmali, I. Erturk and C. Ceken, "Securing Data Transfer in Delay-sensitive and Energy-aware WSNs Using the Scalable Encryption Algorithm," 2009 4th International Symposium on Wireless Pervasive Computing, 2009, pp. 1-6, doi: 10.1109/ISWPC.2009.4800606.

[14]. Daozong Sun, Weixing Wang, Jianqing Lu and Zuanhui Lin, "Design of WSN nodes and network performance analysis in a tea plantation," IET International Conference on Wireless Sensor Network 2010 (IET-WSN 2010), 2010, pp. 144-147, doi: 10.1049/cp.2010.1043.

[15]. Yang Zhang, Sanfeng Zhang, Yi Ji and Guoxin Wu, "Intravenous infusion monitoring system based on WSN," IET International Conference on Wireless Sensor Network 2010 (IET-WSN 2010), 2010, pp. 38-42, doi: 10.1049/cp.2010.1024.