Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 05, pp.50310-50313, May, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

A SURVEY: TO SECURE THE SENSOR NODE DATA IN WSN USING CRYPTOGRAPHY ALGORITHM

***[1]Anushka Tyagi, [1]Gaurav Kr. Singh and [2]Dr. Vishnu Sharma**

[1]M TECH (SCSE), GU, Greater Noida, UP
[2]Professor in SCSE Department, GU, Greater Noida, UP

ARTICLE INFO

Article History:
Received 28th February, 2017
Received in revised form
20th March, 2017
Accepted 07th April, 2017
Published online 23rd May, 2017

Key words:

WSN, Security,
Cryptography etc.

ABSTRACT

Primary WSN are organism positioned for a widespread range of use. It has significant issue to discover out applied safety protocols for WSN due to restriction of authority, calculation and storing properties. Advantage of symmetric key methods is providing better accuracy due to its energy efficacy. But then the disadvantages of symmetric key methods are obvious in standings of key controlling and safety. The Public key substructure is measured to be not appropriate to give security for WSNs as of difficulty. In this paper, we review on key management, storage requirement and security. The large number of new applications for wireless sensor networks has led to unprecedented growth of wireless sensor networks.

Citation: Anushka Tyagi, Gaurav Kr. Singh and Dr. Vishnu Sharma. 2017. "A survey: To secure the sensor node data in wsn using cryptography algorithm", *International Journal of Current Research*, 9, (05), 50310-50313.

INTRODUCTION

Today WSN is an emerging method which connects with each other and with the base position. Wireless sensor network is known as bunched nodes. These systems are normally valuable in numerous fields like soldierly and healthiness. Particular features of the device bulges are condensed power, compact band width, recollection size and lesser energy (Abdoulaye Diop, 2012). WSNs are controlled due to abridged bandwidth, liable to to attacks, collisions in network. There need be specific appliance to create wireless node safe.

Security in WSNs

Safety of Wireless detecting component network has established a significant anxiety of manufacturing. So, it's indispensable to progress the security of WSN meanwhile they're rummage-sale at huge scale. It is not recognized beforehand that nodes are successful to be in message sort of respectively other. To escalation the security of sensor nodes, it is required to put on encryption between sensor nodes (Abdoulaye Diop, 2012). Key organization will increase network safety and construct network resilient beside attacks on it. The earliest network security method is not suitable for noticing module networks attributable to its dignified calculating power and closet astronomical.

Corresponding author: **Anushka Tyagi**
M TECH (SCSE), GU, Greater Noida, UP

All the safety needs cannot be fulfilled concluded a single key scheme as in WSN inconsistent types of messages are dissimilar having totally different requirements for safety. WSNs faces safety threats so there is it want altered key association schemes for WSNs for the motive that maximum no. the beating protocols for WSNs accountable to rationally security compulsions. Key executive is active to form information safe in sensor webs. Key technique in wireless classifying constituent net is firm. Wireless distinguishing part network includes of huge array of sensing component nodes with completely different hardware purposes. Compound security measures can't be working in sensing helping networks temporarily sensing component nodes have controlled memory possessions and condensed energy. Therefore, an energy inexpensive key management subject is serious to alleviate the security risks.

Security necessities in WSN

The objective of safety facilities in WSNs is to defend the info and properties from attacks and misbehavior. The safety desires in WSN comprise:

Confidentiality

Privacy is hiding the data from unconstitutional entrance. In numerous requests, nodes connect enormously subtle info. A sensor scheme should not seepage sensor clarification to neighboring schemes. Modest technique to save delicate data secret is to encrypt the information with a secret key that

individual the predictable receivers 'possess, advanced understanding confidentiality. For instance, public key cryptography is too costly to be used in the source controlled sensor systems; maximum proposed processes procedure symmetric key encryption methods. For symmetric key technique, the key dispersal device should be exceptionally robust.

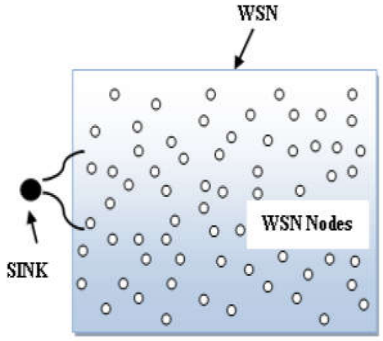

Figure 1.1. Architecture of WSN

Authentication

Substantiation/authentication confirms the dependability of the message through categorizing its foundation. In a WSN, the difficulties of authentication should explosion the succeeding supplies (Matt Welsh, 2003), connecting node is the unique that it assertions to be(ii)the receiver should authorize that the recognized packets have certainly come from the actual sensor node**.** For Confirmation to be attained the two celebrations should part a secret key to calculate message verification code of all associated info. The receiver will approve the authentication of the conventional communication by using the MAC key.

Integrity

Reliability/Integrity is inhibiting the data after unapproved modification. Files confirmation can contribute data dependability also.

Availability

Obtain ability/Availability ensure that services and data can be opened at the time they are compulsory. In sensor set-ups are many risks that could significance in damage of availability such as appliance node taking and denial of service attacks**.**

Cryptography

Cryptology consequent its designation as of a Greek word explicitly "Krypto's" which earnings "Hidden Secrets". Cryptography is the working out and study of hiding info. It is the science of changing basic understandable records dependent to impenetrable info and once more retransforming that communication into its creative form. It sends Privacy, Integrity, and Accuracy

Cryptography Algorithm

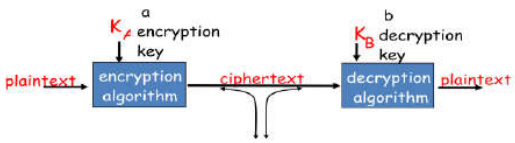

Figure 4. Cryptographic components

Suppose presently that "a" wants to determination a message to "b". Ad's communicated in its single system (for instance, "b", hello. "a") is known as plaintext, or clear text. "a" encrypts his plaintext message using an encryption process so that the programmed sense, recognized as cipher text, expressions unintelligible to numerous interloper. Stimulatingly, in numerous present cryptographic scheme, counting those secondhand in the internet, the encryption technique itself is known-published, consistent, and available to everybody (for specimen, [RFC 1321; RFC 2437: RFC 2420; NIST 2001]), level a possible intruder! Apparently, if everyone identifies the method for instruction files, then there important is convinced secret indication that averts an intruder from decrypting the conveyed data.

Cryptographic Techniques

To choose the greatest appropriate cryptology method is important for the reason that cryptography confirms entirely the safety requirements. To encounter the checks of sensor nodes Cryptographic approaches are used in wireless sensor network must be projected through cipher dimension, information dimension, dispensation time, and influence ingesting. The computational capacity and memory capabilities of sensor nodes are limited, so the traditional cryptography methods cannot be basically moved to wireless network. Therefore, to achieve the safety necessities, whichever the present techniques have to be adapted or novel techniques have to be established. We can categorize them into 4programs based on the present cryptographic methods: symmetric cryptography secret is required. There are number of secret sharing systems procedures, asymmetric cryptographyis accessible such as out dated underground distribution, techniques and hybrid cryptographic techniques and secret sharing.

Symmetric Cryptology Approaches

In this method aimed at together encryption and decryption, a lone common key is used among the two communicating nodes. It is quite solid to save the secret key in a system that uncovered setting wherever WSNs are used. Most security schemes for WSN use only symmetric cryptography, due to its ease of implementation on limited hardware and insignificant energy difficulties.

Asymmetric Cryptology Approaches

In this method, a public key will be castoff to encrypt and verify information and a private key can be used to decrypt and signal information. The isolated key not necessity as revealed although the community key can be obtainable effortlessly. Asymmetric cryptology is too called as Open key cryptography. PKC inclines to be reserve exhaustive, as furthermost schemes are based on huge integer mathematics. Numerous investigators unwanted public key cryptography as infeasible in the incomplete hardware castoff in wireless sensor network for a amount of years for public key procedure methods, like as the Diffie-Hellman key agreement protocol or RSA signatures the code size, data size, processing time, and power consumption make it undesirable, to be employed in WSNs. ECC needs less drive than RSA.

Litrature Survey

In (Panda, 2015), implementing an encryption algorithm by using AES hasbeen planned to deliver for data discretion in a

wsn. It focused on an AES-based symmetric key approach that shares the same key for encryption and decryption among both edges of communication. This procedure consequence in plaintext by manipulative 10rounds mathematically to produce the cipher text in a short period of time.

In (Sekhar, 2012), a procedure founded on PKC (public key cryptography) for outside mediator verification and session key founding has been planned. An external agent communicates through a public key encryption method with a base station, which connects with sensor nodes finished distribution of a private key. The procedure for this protocol is fragmented down into three stages: registration, authentication and session key establishment.

In (Praveena, 2016) proposed well-organized cryptographic method to secure the data in WSNs with the help of Modern Encryption Standard Version-II is presented. MES V-II proposes a type of symmetric key encryption. This process, established by Nath et al., uses the DJSA and TTJSA algorithms in arandomized technique. In this method, a generalized and improved Verna secret message technique is used with different block sizes and secrets for each slab. As an additional security criterion for this algorithm, feedback is also added to this technique. Afterward the nonstop phase encryption is completed, the whole file is separated into two switched parts and the revised Vernam cipher technique with response and a novel significant will be recurrent. Reiterating this whole process a no. of times consequences in a system that is highly secure.

In (Celestine, 2015), a flooding method routing technique is introduced that be determined through on dummy information bases. The foremost knowledge after this method is that every node can be considered as a dummy data source that sends real data after sensing an event to the destination node; totally of this node's neighbor nodes will obtain imitation information. Though this method has the benefit of creation it problematic for an adversary to distinguish between the real packet and imitation ones, it indications to imitation traffic and power feasting as a consequence of this. A novel solution is proposed by using variable sized dummy packets. The pretend packets will differ in size after the actual packets, consequently saving energy; though, an opponent wills motionless invention it problematic to distinguish the real packet from the dummy ones.

In (Prathap, 2016), a solution is projected for gathering malicious nodes with confidence sustenance in WSNs this boards exact WSN attacks by malicious node, including packet adaptation, packet reducing, Sybil Attack, packet misrouting and bad-mouthing incidence. CMNTS recruits the procedure by making a parent-child tree comprises connected information in a sink node. In (Golle, 2004), given secure conjunctive keyword Search done Encoded Files. The location inside which a user provisions encrypted forms (e.g. e-mails) on auspicious site. Therefore to repossess with IDs sustaining a precise search standard user suggestions the web a competence that authorities the site to spot exactly those forms. Effort in this part has for the highest portion focused on search values covering of an individual key. If the operator is really absorbed in forms containing each of numerous keywords (conjunctive key search) the operator should whichever offer the server competences for each of the keywords separately and trust on an connection control (by any the server or the user) to determine the correct set of documents, or alternatively, the user might store extra information on the web to simplify such searches.

In (Vimal Upadhyay) were industrialized protected files in WSN through DES. It is unique in all the furthermost goals of sensor networks are to create correct data a combine of detecting ground for aprolongedera of period. The appearance of sensor grids together of the important information progresses confidential the recurrent eras has defenseless numerous characteristic experiments to investigators. Region behind sensor systems act as penetrating information and or operate in aggressive unattended surroundings, it's authoritative that these safety deliberations be speak to from the commencement of the organization design. These systems are perhaps to be collected of hundreds, and potentially thousands of little sensor nodes, functioning autonomously, and in several cases.

In (Sadaqat Ur Rehman, 2012), presented Evaluation Constructed Investigation of many Cryptology and Encryption Methods using MAC in Wireless Sensor. In WSNs have develop mutual day by day, but one between the greatest problem in wireless network is its limited properties. The properties to create MAC observance in mind the feasibility of way used for the sensor network at pointer. This investigation effort examines totally unrelated cryptographic approaches likes' symmetric key cryptography and asymmetric key cryptology. Still, it associates dissimilar encryption methods such as stream cipher (RC4), block cipher (RC2, RC5, RC6 etc.) and hashing techniques (MD2, MD4, MD5, SHA, SHA1 etc.).

In (Anderson Santana de Oliveira, 2012), was presented Privacy-Preserving Methods and Organization for Flowing Files in 2012. In this projected effort measured great enactment symmetric encryption methods for greater-than and variety inquiries founded on Bloom sifts; a scheme application of privacy-preserving time association based on MX-Query [maximum query] and a systematic presentation assessment of symmetric encryption methods permitting parity tests, range queries, and shade accumulation.

In (Fei Chen and Alex X, 2012), accomplished Confidentiality and Reliability Preserving Choice Inquiries in Sensor Networks in 2012. In sensor systems storing node purpose performance as atransitional among sensor and a sink for storing data and dispensation inquiries. It has been extensively accepted since of the assistances of power and storage saving for sensors as well as the competence of query processing. The problematic of this method is the assailants hack the storing node. To avoid attackers from a head info from both sensor collected data and sink issued queries. The encryption procedure is introduced use to encode each data and queries specified by a storage node. This properly by using data encryption standard algorithm. Data encryption standard procedure is not applicable for better security in sensor collected data and sink issued queries. Because, future work will use RSA procedure to protect data and enquiries.

Challenges

- 1One of the main issues of the placement of MAs in wireless network contains protected broadcast of

mediator as well as inhibiting unapproved access to assets among interactive sensor bulges.
- One more big challenge for disposition of symmetric key cryptography is how to resolutely assign the common key among the two interactive clouds.
- Unique specific challenges to protected routing in WSn are which is very informal for a distinct node to disturb the defeating procedure by distracting the way location procedure.
- The challenges to be fetches in WSNs are reporting and arrangement, scalability, QaS, size, estimation control, power ability and safety.

Application

- Wireless sensor network is frequently use in the application of assembly of info from the nearby situation, so it is essential to defend the subtle data from unapproved events.
- The leading part of sensor system in safety for numerous applications be determined by on secure routing.
- So safety resolutions for numerous uses are built on symmetric key cryptology.
- Wireless sensor network (WSN) is employed in many application areas such as monitoring, tracking, and controlling.
- WSNs is a collected of no. of sensor bulges in a large number of application such as military, airspace, temperature, light , humidity and then communicate with each sensor in wireless networks.

DISSCUSSION

In beyond numerous works in literature survey accessible by numerous Authors, we examine about various or many present research idea in terms of concept of the Wireless sensor networks, Cryptographic algorithms, Sensor nodes and Energy Efficient Cryptographic (EECA) algorithm .It is a significant contest to discovery out appropriate cryptology for WSN due to limits of power, calculation competence and storing capitals. Numerous systems grounded on public or symmetric key cryptology are examined. Recently, an applied identity-based encoded technique is planned. WSN is an extensive development part for precisere serve in complete use. Feature related with knowledge like, the encryption safety, working speed and power consumption for system. Now, we present a mechanism for secure transferring of data is WSN and various security related issues. Safety is measured to be a significant issue in WSNs. Clustering is ineffectual and suitable way to improve presentation of the WSN scheme. Sensor nodes have imperfect power, computational capabilities and recollection. Cryptology is the maximum offered safety service in wireless sensor network.

Conclusion

The WSNs remain to produce and develop extensively used in numerous presentations.

So, the essential for safety develops vital. This paper have focused on Symmetric Cryptology due to the supposition that symmetric cryptology has a advanced efficiency and need less energy consumption, in difference to public key cryptosystem.

REFRERENCES

Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain, "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks*", International Journal of Computer and Communication Engineering*, Vol. 1, No. 4, November 2012.

Anderson Santana de Oliveira, Hoon Wei Lim, Su-Yang Yu " Privacy-Preserving Techniques and System for Streaming Databases" in 2012.

Celestine, J., et al. An energy efficient flooding protocol for enhanced security in Wireless SensorNetworks. in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island.2015. IEEE.

Fei Chen and Alex X. Liu , "Privacy and Integrity Preserving Range Queries in Sensor Networks" in Dec. 2012. Networking, IEEE/ACM Transactions on (Volume:20 , Issue: 6)

Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton ―Resuscitation monitoring with a wireless sensor network‖, in Supplement to Circulation*: Journal of the American Heart Association,* October 2003.

Golle, P., J. Staddon, and B.Waters, "secure conjunctive keyword search over encrypted data, " in proc. ACNS,2004,pp. 31-45.

Panda, M. Data security in wireless sensor networks via AES algorithm. in Intelligent Systems andControl (ISCO), 2015 IEEE 9th International Conference on. 2015. IEEE.

Prathap, U., P.D. Shenoy, and K. Venugopal. CMNTS: Catching malicious nodes with trust supportin wireless sensor networks. in Region 10 Symposium (TENSYMP), 2016 IEEE. 2016. IEEE.

Praveena, A. and S. Smys. Efficient cryptographic approach for data security in wireless sensornetworks using MES VU. in Intelligent Systems and Control (ISCO), 2016 10th InternationalConference on. 2016. IEEE.

Sadaqat Ur Rehman, Muhammad Bilal, BasharatAhmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman "Comparison Based Analysis of Different Cryptographic andEncryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)" IJCSI *International Journal of Computer Science Issues*, Vol. 9, Issue 1, No 2, January 2012

Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques. InComputer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.

Vimal Upadhyay, PintuKashyap, Inder Kumar, Jai Balwan , Lalit Choudhary " secure data in wireless sensor network via des" *International Journal of Enterprise Computing and Business Systems* ISSN (Online) : 2230-8849

****