iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

A Novel Approach for Data Security in Wireless Sensor Network using Cryptography

Sanju Paswan[1], Rahul Piwal[2], Vishal Vishwakarma[3], Dr. Bharti Sharma[4]
[1, 2, 3, 4]*Department of MCA, National Institute of Technology, Kurukshetra-136119*

***Abstract:** In this paper, we focus on development an algorithm for the data security in wireless sensor network. Wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. We used cryptography for data security. Cryptography is a technique in which we convert some plain text into some unreadable form called cipher text and make our communication confidential, converting plain text into cipher text called encryption and after being encrypted getting plain text again called decryption. In this paper we implemented Symmetric cryptography approach. Symmetric approach uses single key for both encryption and decryption. we made 8*10 (for encryption and decryption of the data) matrix in order to provide adequate security Moreover using of 8*10 matrix increases adequate security for data since it needs 80 factorial chances to crack. Object of this project is to develop an algorithm which works well with sensor nodes.*

***Keyword:** Wireless sensor network; Security; Energy consumption; Cryptography; Constraints*

I. INTRODUCTION

WSN could be interpreted as area of electronic devices that could address the data collection by monitored areas by sensor nodes. The curious data is forwarded through many nodes. WSN is a wireless area that consists of many places and many nodes. These networks are used to observe physical or environmental situations like voice, pressure, temperature and then pass data through the network to a main destination point. [1] WSN is consist of a extensive number of sensors devices called nodes those create the wireless network using self-preserve, and its main aim is, observation processing and transmit the data those nodes get from the distinct areas. The nodes sink node made the whole WSN. Sensor Nodes are the basic base of the entire network, those are only amenable for cognition of data, process the data, store it and transmission of information. Nodes are fraternal complicity, nodes never uploads the data directly, instead of upload the data directly nodes utilize their own processing potential for operation and unification. The Nodes of sensor collect environmental data, like temperature, humidity, pressure, vehicle motion, mechanical pressure strength, and the motion of the airflow and other things and in many other areas sensors network is very significant as health, military, space and marine survey has been extensively used. In WSN nodes have unpreventable networking function those could report with each other. In the approach of WSN, the nodes are fixed without network facility. As like a huge space of forest or in insecure area where human can't reach there, In that case sensors nodes has the ability to collect the data by their system by itself. When sensor nodes communicate precisely with the gateway, it needs other sensor nodes for transmission of data. So the network for transmission of data should be multi-hop routing and In other applications of WSN. It may stop because of less battery and consumed energy or can be other failure, these points would modify the network topology changes. In WSN we use many nodes and often arranged in a specific monitoring area from there human can't get the data, but sensor nodes has some constraints those degrade the performance of WSN, and in mobile communication network mainly affected that how to enhance the data transmission with present constraints. While designing the network process, our main focus should be that how to get the exact data and transfer the acquired data to user. In the WSNs study for protocol, medium access control and routing protocol is the main pinpoint to know. By this medium access control protocol is a set of rules, straightly and fairly use media. Protocol of Routing only intended to data packets transfer from one node to other then at the destination node in that network, it finish the important explore for best path and transmit information as per the best path. In WSNs generally have problems of battery-powered, low process and many, and after deployment of nodes it is tough and replacement of node also difficult, so as per the security purpose we should use an efficient approach that can work efficiently without any problem. To provide Security to data mainly forced two major points transmission and data security. transmission mainly focuses the secure the nodes and data security mostly focus on the data confidentiality, data integrity .[6]

WSNs is mainly is the combination of layers and these layer are main reason to provide security to sensor from various attacks.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

II. SECURITY REQUIREMENTS

In sensor network data travel from multiple nodes and there might be a chance of the data leak. To provide the data confidentiality an encryption is the way.

A. Data Confidentiality

In sensor network data travel from multiple nodes and there might be a chance of the data leak. To provide the data confidentiality an encryption is the way.

B. Data Integrity

In that case original data is changed by the third party and they can modify the original data according to their requirement and send this new data to the receiver.

C. Data Availability

Data availability means that service of data is available all the times even in case of any kind of attacks such as Denial of service.

III. LITRETURE REVIEW

One way to secure our data is encryption technique, where digital data, storage disk are encrypted and by it we can secure our data from unauthorized access. In a cryptography technique, we convert our data any understandable language which no one can read except those who had encrypted it.

The sensor network suffers from many impactions. It suffers from low battery power, small amount of memory to store the data and computation capabilities. So selection of right cryptography technique is also very significant, that techniques which will work well with its constraints and produce desirable result. For this we have two techniques in cryptography one is symmetric key and other is asymmetric. [6]

A. Asymmetric Cryptography

These approaches we use for encrypt and decrypt the data. This approach works on two pair of key private and public , public key for encryption and for private key for decryption. Both public and private key

should be of receiver then sender use public key of receiver for encryption and at the receiver side, receiver used its own private key for decryption that encrypted data. Some important algorithm of Asymmetric cryptography.

1) RSA (Rivest-Shamir-Aldeman): RSA is an algorithm technique which is used for encrypt and decrypt the data. RSA is based on asymmetric algorithm. In asymmetric key algorithm we use two keys one is private and other is public which gives to everyone. RSA is generally used for a huge integer number to factorization. So if someone wants to factorize the number, we use private key for decrypt.

2) Digital Signature: Digital signature is generally used for the authentication. It ensures that the data which is send by the sender is came by the right person or not. Digital signature is used in electronic mails, e-commerce, and digital market.

3) ECC (Elliptic-curve cryptography); ECC is an application use Public-key cryptography. It is basically works on algebraic form of elliptic curve. It requires small keys to provide security than non-ECC cryptography. It helps for key agreement, digital signature, pseudo random generator and some other tasks.

B. Symmetric Cryptography

This is another approach of cryptography. This approach works with only single key (private key) for both encryption and decryption. Sender first encrypts the data by private key and generates a cipher text and send to receiver then at the receiver side receiver will Decrypt that cipher text by private key. Some important algorithms of Symmetric cryptography.

1) Data Encryption Standard (DES): DES is a data encryption algorithm which is very common for encrypt the data. It makes a form of secret key, which is used for encrypt and decrypt the data. In public key we have two keys one is for encrypt the data and other is for decrypt the data.

2) Caesar Cipher: The caeser cipher technique is very easiest technique to use for data encryption. In Caesar cipher a text message is shifted by a certain number.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

IV. COMPARITIVE STUDY

Constraints (low battery power, small amount of memory to store the data and low computation capabilities) of WSNs are one of the main issue for security, for encryption there are three encryption standards, asymmetric approach, symmetric approach and hybrid approach, but Asymmetric encryption algorithm Which generates the big cipher text which requires big processor to process basically it will effect node's all constraints which degrade the security of data And on the other hand Symmetric and hybrid encryption algorithm generate small cipher text and work which is easy to any sensor node to store and process data. This is the comparison table among algorithms of symmetric and asymmetric approach

S.NO	Algorithm	Packet Size(KB)	Encrypt Time (Sec)	Decrypt Time (Sec)	Buff Size
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934
5	DES	312	3.0	1.6	319
	AES		1.8	1.3	300
	RSA		7.8	5.1	416

Table-3

©IJRASET: All Rights are Reserved

Factor	Play Fair
Invented	1854
Key Size	25!
Algorithm	Symmetric
Encryption	Faster
Decryption	Faster
Power Consumption (mw)	
Small (1 MB)	11.3
Medium (10 MB)	35.6
Large (1GB)	42.
CPU Time (ms)	
Small (1 MB)	6.2
Medium (10 MB)	21.3
Large (1GB)	31.6
Transmission Time (ms)	
Small (1 MB)	12.8
Medium (10 MB)	39.2
Large (1GB)	50.6
Ciphering & Deciphering Algorithm	Different

Table-4

V. GAPS

Protocols in WSN are working well but they consume lots of energy and space, so low battery consumption, low processor, and small storage area are the problems with WSN. Because after encryption the out can be big which may require big processor and memory .So we have to protect for these things during work with WSN security. Any tampering with WSN constraint can affect its performance and can give the undesirable result. [1,5].

VI. PROPOSED SOLUTION

So from the above comparison table which shows that algorithms of Symmetric approach are being working well with Sensor and give adequate consistence to network. Even though Existing protocols are being working well however they give unpleasant effects on WSN constraints, Selection of protocols is also important because they needs to be work well with its constraints and give desirable results. keeping in mind its constraints the symmetric approach is being give pleasant results. So our algorithm follows Symmetric approach (single key for both encryption and decryption),in which we are using 8*10 matrix as a single key for encryption and decryption. This 8*10 matrix increase more security since 80 factorial chances to be needed to cracked by Brute force approach.

©IJRASET: All Rights are Reserved

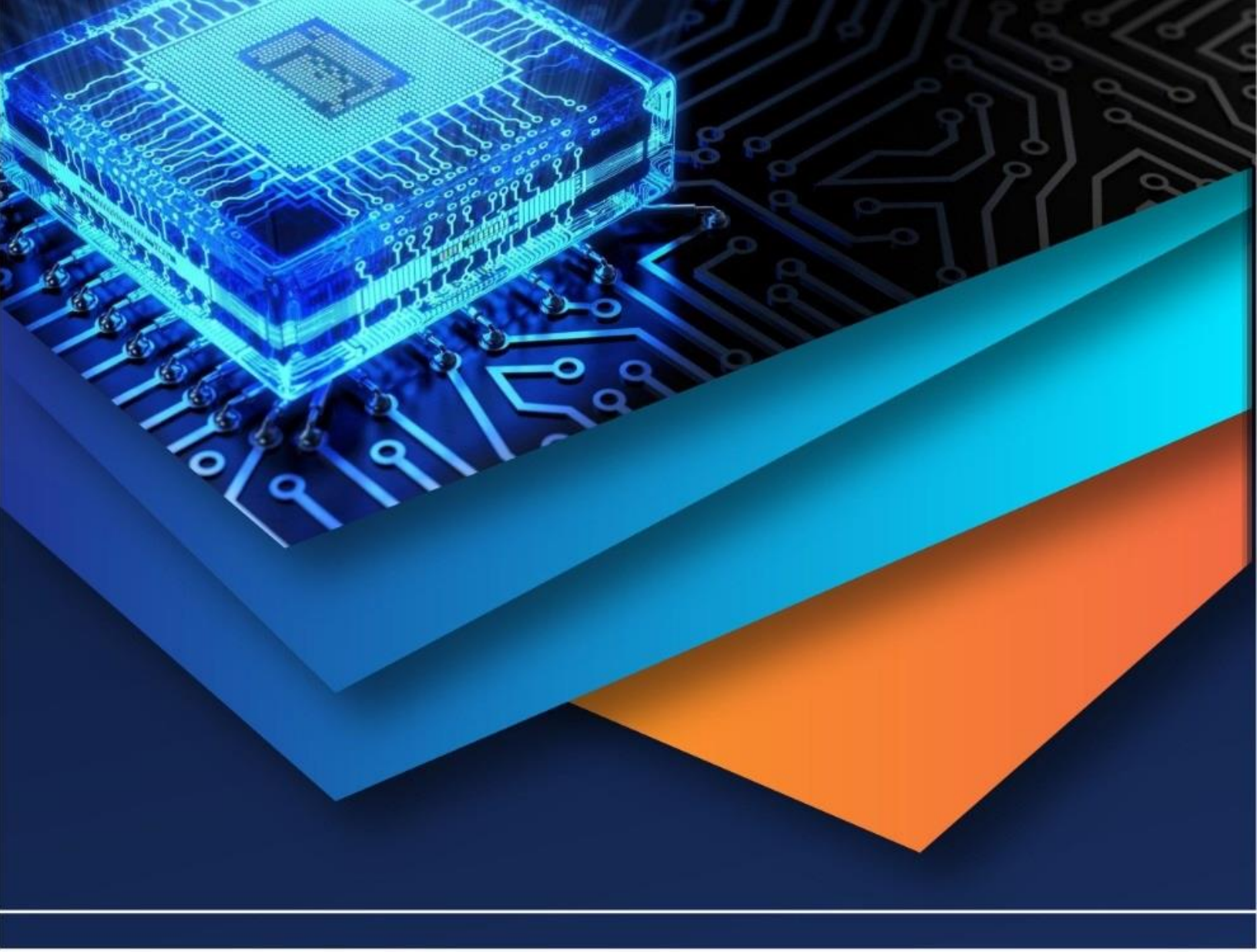
VII. CONCLUSION & FUTURE SCOPE

In this paper we have identified some constraints of WSNs (like low battery, low storage, low space) Which degrade the performance of WSNs and got that Symmetric approach would be better than Asymmetric approach, and compare the performance of some algorithms from both the approach by which we got that result of Symmetric one is better. Then got that effects of adequate efficient aggregation technologies which focus to improve power efficiency and found that Only data security in WSN is not enough, securing data from malicious node is also significant as much as select efficient algorithm and week protocols those degrade the security performance and increase unacceptable risk for data, all routing protocols on Network layer how generally look security and how week routing protocols could be a reason of lost the data packet, and got that protocols of Application Layer which implements Authentication and provide security by Password, biometric and user face recognition. Week protocols of Application layer may lead to Attacks. So this paper conclude that these things can provide adequate security to our sensitive data but for Military where data is major concern need more securer protocol at every layer, and the algorithm which we gave is also follows the symmetric approach and using 8*9 matrix increases the chances of more security'

REFERENCES

[1] Parli B. Hari, and Dr. Shailendra Narayan Singh, "Security Issues in Wireless Sensor Networks: Current Research and Challenges", (2016).
[2] Jingcheng Zhang, "Wireless Sensor Networks", (2014).
[3] Ian F. Akyildiz and Mehmet Can Varun "Wireless Sensor Networks", (2016).
[4] Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", (2014).
[5] Yan-Xiao Li, Lian-Qin and Qian-liang, "Research On Wireless Sensor Network Security", (2015).
[6] Alexander Betts, Frank Meyer-Bodemann, Fred Muller and Shao Ying Zhu. "Wireless Sensor Network Security: A Critical Literature Review", (2016).
[7] Haythem Hayouni, Mohamed Hamdi and Tai-Hoon Kim, "A Survey on Encryption Schemes in Wireless Sensor Networks", (2014).
[8] Tanveer Zia and Albert Zomaya, "Security Issues in Wireless Sensor Networks", (2015).
[9] Gurudatt Kulkarni, Rupali Shelk , Kiran Gaikwad, Vikas Solanke, Sangita Gujar , Prasad Khatawkar, "Wireless Sensor Network Security Threats", (2016).
[10] Sanjeev Setia, Sankardas Roy and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Network", (2015).
[11] P.uthaya bhanu, J.saravanan, "Data Security in Wireless Sensor Network", (2014).
[12] Tarikul Islam, Subhas Chandra Mukhopadhyay, Nagender Kumar Suryadevara, "Smart Sensors and Internet of Things: A Postgraduate Paper", (2017).
[13] Santar Pal Singh, S.C. Sharma, "A Survey On Research Issues in Wireless Sensor Network", (2015).
[14] Aiman Faquih, Priyanka Kadam, "Cryptographic Techniques For Wireless Sensor Network: A Survey", (2015).
[15] Jintender Grover , Shikha Sharma, "Security Issues In Wireless Sensor Network", (2016).
[16] Xiaojiang Du, Hsiao-Hwa Chen, "Security In Wireless Sensor Network", (2015).

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)