iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: IV Month of publication: April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4176

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 IV, April 2018- Available at www.ijraset.com

Review Paper on Data Security in Wireless Sensor Network

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

Abstract: The extensive use of WSNs in many applications increases the security concern for data. Implementation for security solution is major issue for this network with tiny sensors node those all have major constraints i.e., low computation, low battery, low space and low memory. This paper shows major things for security those we got from after analyses the important security issue and confer the other important aspect for furthermore enhancement to developer in their efforts to create the most potent and suitable method for secure network. This paper, mainly focus on the data security of WSN, that what are the possible way to provide security to data in WSN and identify some gaps/problems those are the inhibition of security in WSN. To overcome these gaps there are possible techniques and found the problems with existing technologies. To secure data from attack, this paper provide some significant things those are important for security purpose in WSN.

Keyword: Wireless sensor network; security; energy consumption; Cryptography; constraints.

I. INTRODUCTION

WSNs 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]

WSNs 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 WSNs. 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 WSNs nodes have unpreventable networking function those could report with each other. In the approach of WSNs, 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 WSNs. It may stop because of less battery and consumed energy or can be other failure, these points would modify the network topologies changes. In WSNs 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 WSNs, 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.

II. SECURITY

A. Layered Security Model

WSN has many difficulties in security, some of these are, dynamically alter the topology, WSN is surrounded by the nodes and its hardware has some constraints those directly affect the security like memory capacity, energy source and low communication bandwidth.[15]

APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL

III. 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.

IV. WSN NETWORK TOPOLOGY

To establish WSN we can use some topology.[2]

A. Star Topol Ogy

In start topology each node dedicatedly connected with gateway. Gateway control the all data flow in star topology. Gateway directly sends and receives the data from the other connected node. For communication with other node, first they have to send the data to the gateway the gateway send the data to the other intended node. [2]

B. Tree Topology

Tree topology is formed as a tree. Every node is connected to the root node and every root node has its left and right child .In tree topology every top root node directly connected with the gateway.so in tree topologies data travel in a systematic way. In tree topology we can expand our network easily and we can find any error then solve it easily. The disadvantage with this network is that it totally based on the bus cable; if it breaks, all the network will shut down.[2]

C. Mess Topology

The Mesh topology is a collection of node in which data travel only node to node .if one node want to communicate with other connected node and they are not connected so data will travel by its interconnected node. Fault detection is easy in Mess topology. The disadvantage is that the network is large require big investment.[2]

D. Bus Topology

A bus topology is a multipoint topology, in that the nodes get connected with a single cable , the cable act as a backbone , all the data travel with the help of that cable and reach at the destination point.

V. SOME OTHER ISSUES IN SECURITY

A. Routing Protocols

1) *Significance of Routing Protocols:* Routing protocols are the major point to transmit the information on network, and during transmission it requires efficient security technology is on major concern of the protocols. Weak routing protocols can degrade the security of data. An adequate secure routing protocols play a significant role in data security of wsn, and as per the constraints protocols must consume less energy and it can be possible to fix the weakness after routing protocols has been designed.so consequently while designing the routing protocols we must keep the objective in mind. [8]

B. User's Authentication

1) *Significance of User authentication at application layer:* Application layer add the protocols which connect the users and defined that how will user get connected with that network, and in sensors network this mainly establish for user authentication with the network, conventionally sensor network authenticate the users by GW devices, and after the growth of WSNs authentication of users is done by sensors to collect real –time data. This section finds the more efficient protocols prevent the unauthorized person on WSNs network; those are password based, smart card based and biometrics based authentication.[9]

C. Malisious Node

WSN are unsafe across from many attackers. Attackers can easily add some malicious node in the network and can easily steal the important data. In sinkhole attack, a malicious node can act like fraud data to attack on network and get that data. It claim and shows tiny path toward the sink node so that other sensor nodes attracted towards to it. For data transferring mostly routing algorithm selects shortest path to send the information.[13]

D. Data Aggregation

Data aggregation uses to reduce the power consumption. It is used to combined and summarize the data packets of several nodes to reduce the data transmission. It reduces the number of data transmission to for improving the energy utilization and bandwidth in WSNs.

VI. MOTIVATION

WSN provide some characteristics those very helpful for humans. That are-

A. Flexible

WSN is very flexible.it can change in any changes with any harm.

B. Additional of new device

We can add any device in WSN easily without interrupt the hole network and remove the damage device easily.

C. Save Cost

WSN reduce the wire expenses and by this we can save our lots of money.

D. Useful to Society

WSN helps humans in many fields like healthcare, defense and environment monitoring. Most of the applications take use of wireless sensors network that's why making the data coming from sensor needs security. [3]

VII. 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 cryptographic 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 cryptographic 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, pseudorandom generator and some other tasks.
4) *ElGamal:* In cryptographic technique, the ElGamal technique is an Asymmetric cryptographic technique which is used for public key cryptography.
5) *DSA (Digital Signature Algorithm):* It is a technique for generating and validating digital signatures. Basically it provides integrity of data and non-repudiation and content of a digital messages.

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 caser cipher technique is very easiest technique to use for data encryption. In Caesar cipher a text message is shifted by a certain number.

3) Rail fenc: -In rail fence technique, the text message is not changed, but the positions of the texts are switched to their original position. It is also called a transposition technique. In rail fence technique we arranged the original texts in zigzag form. To encode the code we just take top line value and combine them. Similarly with the bottom line value. Then we got the encoded form of the original text.

In hybrid approach we use both keys, but encrypt of data is done by random symmetric key than with and then we encrypt that symmetric With the help of receiver's public key and then send that encrypted data with encrypted symmetric key to destination point, and at the receiver side, Receiver first encrypt that symmetric key (by which we encrypted our data) By their private key and now receiver has its symmetric key by this he can decrypt that encrypted data. [4,7]

VIII. 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.

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

These are the some factor by which we can conclude that symmetric approach is better than asymmetric approach in while working on WSNs.

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

IX. 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. 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].

Processor	4 MHz with 8- bit
Primary Storage	8K Instruction flash 512 bytes RAM 512 byes EEPROM
Communication media	916 MHz Radio
Bandwidth in Kbps	10
Operating System	Tiny OS
OS Code	3500 bytes
Availability of code space	4500 bytes

X. PROPOSED SOLUTION

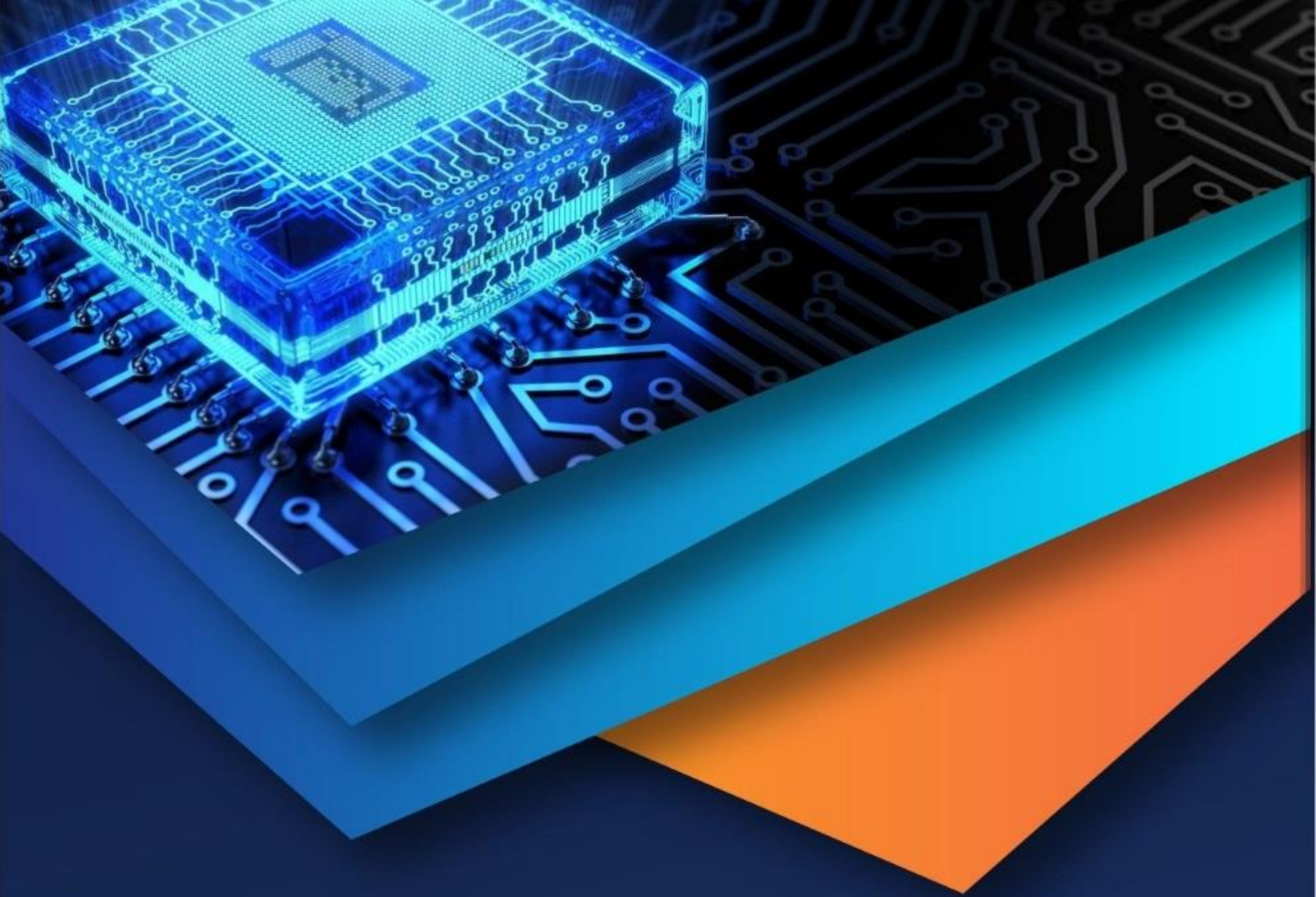
Existing protocols are working well however they give unpleasant effects on WSN constraints. During work with protocols, we have to designed the protocols in that way so they work well with its constraints and gave desirable results. The symmetric approach is the way which works well in WSN and gives appropriate security to our data from an unauthorized person.[4,7]

XI. CONCLUSION

In this paper we have identified some constraints of WSNs (like low battery, low storage, low space) Which degrade the preformation 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.

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).



doi crossref

10.22214/IJRASET

INDEX COPERNICUS

45.98

ISRA JIF

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY