Comparative Analysis of Hash Function and Symmetric Algorithm for Data Security in Wireless Sensor Networks

Chanchal Sharma
Research Scholar (M.Tech)
Krishna Engineering College Ghaziabad, India

Vinit Kumar, PhD
Associate Professor
Krishna Engineering College Ghaziabad, India

ABSTRACT
Wireless Sensor is utilized as a part of numerous territories, for example, controlling, checking following. System security is a vital assignment that must be extremely considered when outlining a system. It is characterized as a methodology and process took after by a system head to ensure the system gadgets or the information from undesirable dangers and unapproved clients. System security is the imperative part in data security since it is in charge of securing all information went through system. In current period arrange security has turned out to be more critical for exchange of information starting with one PC then onto the next PC, in each association and the military. With the advancement of web security turn into a noteworthy worry for secure the vital information. Due to quickly expanding no of PC's in associations numerous systems has been built up. As per expanding of no of system and clients on the planet and increment the no of dangers and unapproved client that is the reason the system isn't sheltered and we required a security on the system.

Keywords
Wireless sensor network, Data encryption algorithm, MD5, SHA-1.

1. INTRODUCTION
Presently a day's system security is a critical worry for the data security. System security is fundamental for each system since data is passed on the system amongst PCs and the switches. Everybody have been shielding their information from the dangers and infection by utilizing distinctive kinds of security however such security strategies recognize and hurt the data, that is the reason we required greater advancement in security techniques. Web has turned out to be for the most part spread all over, if any unapproved element need to gain admittance to this system, he can hurt us as well as he can without much of a stretch assemble all the data about us. System security is a strategy by which we ensure information over wired or remote system. System security required in each place either opens or secret that is uses on every place private companies as well as government offices. System security comprise the standard and decide that is given by arrange overseer to anticipate and screen unapproved access, abuse and adjustment of information. For the security of data on remote system or wired system we needs information ought to be classified, shielded from any unapproved change and safely accessible when we need to utilize it. When we make organize or work a system we ought to comprehend the significance of security arrangement. The fundamental motivation behind system security is to ensure against undesirable assaults. There are different kind of system dangers and assaults are accessible that is the primary worry for remote systems administration and wired systems administration. System security is an approach to keep the information on arrange. In which come both equipment and in addition programming innovations.

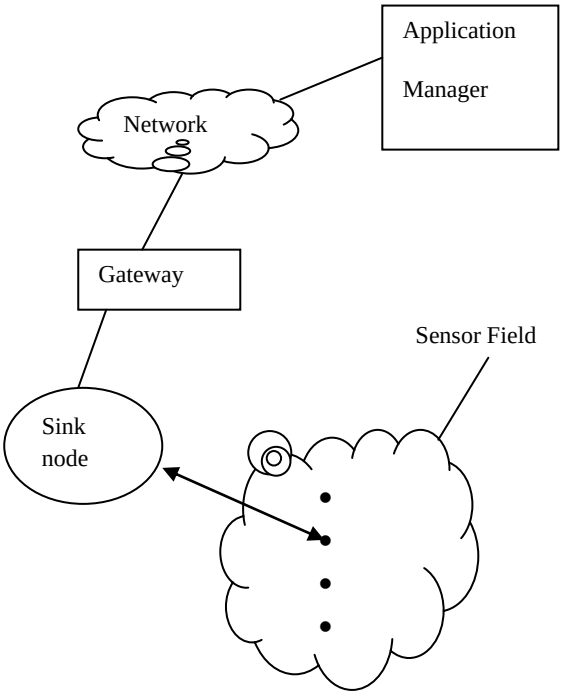

Fig 1: Architecture of WSN

In this paper we present the security mechanism of WSNs. In section 2 presents the literature review. In section 3 Presents the problems and issues in wireless sensor network. In section 4 present the attacks in network security. In section 5 present the security requirements and in section 6 and 7 presents the result and conclusion of security in WSNs.

2. LITERATURE REVIEW
System assaults on Wireless sensor systems have been distinguished to be as differed in structure that they undertaking to get it. Unknown attacks either outlined on the important data of the organization that is secured for replacement of some data by admin or other necessary use. In this paper shows that how any intruder takes attack on the important data and policies of securing that data. Day by day attacks are increasing on the data and system specialist finding multiple attacks in the organization that is harmful for admin as well as company.

2.1 Earlier Network Security Basic Tips
System Security helpful safety measure strategies to secure system, for example, introducing a refresh antivirus program, email examining programs, organize observing instruments, we get to arrangement and other security counteractive action techniques. System security is the most fundamental segment

in data security since it is in charge of ensuring all data went through system. System security is an essential type of a PC arrange. Minor security weakness can bring about a substantial loss of the basic information of your server and other customer PCs. System overseer is mindful to secure the data on the system. There are part of security size and anticipation techniques those will be examine in this area. Ordinarily a PC system can be assaulted by various routes, for example, infection assaults, unapproved get to, and various other security dangers. Consistently examine all the system gadgets, messages, open ports, server and customer PCs. It's the duty of the system managers to check and expand the missing security lump in every one of the PCs. They ought to likewise expel the superfluous system shares, client's records; remote access indicates and limits the entrance the system clients. These are following basic network security tips.

- Turn off ping Service
- Close unused port
- Use intrusion detection system and intrusion prevention system
- Firewalls

2.2 Types of attack in Wireless sensor networks

2.2.1 Denial of Service

There are numerous security dangers that can be the reason for a system security assault. In which security dangers are refusal of administration, conveyed dissent of administration, infections, Trojan steeds, spywares, malwares, unapproved access to the system assets and information, and unplanned cancellation of the documents. It happens by the surprising disillusionment centers or undesirable work. The minimum troublesome DoS strikes try to leak the benefits open for setback center, by sending additional futile packages. DoS attacks is inferred not only for foe's undertaking to bother, or crush a framework, yet what's more for any moment that decreases a system's capacity to give an organization.

2.2.2 The wormhole attack

One centre point in the framework (sender) establishes a connection on the centre in the framework (gatherer hub). At that point the tolerant centre undertakings to send the message to its neighbours. The neighbouring centre points think the message was sent from the sender hub, so they attempt to send the message to the starting centre point, yet it never meets up since it is too far away. Wormhole strikes is an essential risk to remote sensor frameworks, since, this sort of ambushes does not require exchanging off a sensor in the framework rather, it could be performed even at the hidden stage when the sensor start to discover neighbouring information. Wormhole strikes are difficult to counter in light of the way that controlling information give by a centre point is difficult to affirm.

2.2.3 The Sybil attack

This assault is a single center i.e. a pernicious center will give off an impression of being a course of action of centers and will send wrong information to a center in the framework. The wrong message could be a collection of objects, location of center points, characteristics of center points that don't exist. Affirmation and encryption framework would safe be able to dispatch a Sybil danger on the sensor sorts out. In any case, an insider can't be kept from appreciating the framework, in any case, just barely has the ability to do in that capacity using the characters of the center points he has exchanged off. Open key cryptography can turn away such an insider assaults, yet it is too expensive to ever be used as a piece of the advantages constrained sensor systems. The system assets and data ought to be getting too just to the approved people.

2.2.4 Passive information gathering

In passive information gathering intruder takes attack on the main centre where data gathered. In this attacker collect the data of the organization and use that data for unwanted place. The centre of the data gathering by the user gives the potential to the unauthorized user. This type of attacks is dangerous for the organization.

2.3 Goals in network security

These are the following goals in network security

- In confidentiality, the sender and the beneficiary ought to have the capacity to get to the substance of a message. Classification is intended to keep delicate data from achieving the undesirable dangers. Confidential data only get by the authorized user. In this who wants to get access then there is many types of enquiry should be available. It is useful for those individuals who have the lots of important data..
- Integrity means maintaining the stability of data. Main purpose of integrity is that the data should not be modifying in the transformation between client and server. By this client can send the authorized information to the user. This is used to prevent the data from unwanted individual. There should be some logic between source and destination, if some unwanted entity wants to modify data then some electric gadget ring the alarm. By using the checksum can analysis the correct form of information. And by using redundancy reestablish the data.
- Availability is used to secure the data from unwanted set up of network, then repair all the network but there should not be any software crash. This is used to maintain full structure of network. It is used to stop all these type of obstacle in the networking. Availability is useful to safe from unwanted change in the information. Security across the data intrusion or data breaking is a challenge for availability. Some extra security for the software as well as for physical things in network such as firewall and some middle things between client and server by these data cannot be able to come on destination.

3. ATTACKS ON WIRELESS SENSOR NETWORKS

3.1 Eavesdropping attack

These assaults comprise of the unapproved hold over of system correspondence and spotting of the traded information. This can be on arranging layer by sniffing into the exchanged parcels or in the physical layer by physically wiretapping the entrance medium. In this attack information can be gathering by video, audio, calls, text and other electronic things. VoIP structure doesn’t use encryption process that’s why intruder easily can attack on calls. When they play with TDM calls with that notice IP calls as well and catch them. By custom authority can pick up the random call and judge that call. In that some logic behind that calls such as in backend process

they change the logics and changes CODECs into WAV file. They can listen all the calls without any permission of the user by changing the gadgets [4].

3.2 Logon abuse attacks

Logon mishandles assault would obstacle for verification amongst customer and server and access control system. This is enabling a client to get access with more accommodation at that point approved.

3.3 Spoofing

In spoofing assault a subject stating a personality after then subject has no privilege to utilize. In this kind of caricaturing programmer do IP ridiculing by which they can assault on comfort framework that is in speaking with a known guideline. In which the assailants sends a parcel with an IP source address of a known put stock in have by transport layer. The goal host might be cheated and acknowledge the changed bundle as legitimate. Caricaturing assault is one in which IP address of a parcel is imitative. Fundamentally parodying alludes to stolen data when a man appear as another individual association or business with the reason for increasing individual data including client names and passwords, ledger data and Visa numbers [8].

3.4 Intrusion attack

In intrusion attacks the hacker's center around unapproved clients accessing a framework by the system. In arrange interruption is any unapproved follow up on a system. Finding an interruption relies upon the preserver having an unmistakable of system assaults. In interruption cases, some undesirable movement retains arrange assets cognizant for different uses, and assaults on the system security and information. There are numerous sorts of interruption assaults in arrange security. [1]A framework interruption attack can be utilization of a system that bargains its dependability or the aversion of information that is put away in framework associated with this. In interruption assault unapproved client pick up assaults on records or benefits, or misusing of programming and other information.

4. SECURITY REQUIREMENTS IN WSNs

A WSN is an uncommon type of system. It imparts couple of shared characteristics to a standard networking system, yet additionally displays numerous highlights that are sole to it. The administrations of security must ensure the information imparted over the network and the assets from assaults and nodal unfortunate behavior in a WSN. These are the following essential security mechanism.

4.1 Data confidentiality

The security component needs to ensure that no message in the network is comprehended with the guide of anyone other than gathered beneficiary. In wireless sensor network, dangerous of categorized should place the following necessities.

4.2 Availability

These necessities ensure which the WSN administrations ought to be open constantly even in event of an outer or inner assaults e.g. DoS. Different strategies have been characterized through examiners to achieve this target. While a few instruments make adventure of extra report among hubs, others propose use of a focal access control framework to ensure fruitful exchange of all messages to its beneficiary.

4.3 Data freshness

It infers which the information is present and ensure which no foe can replay old messages. This need is particularly noteworthy when the WSN hubs abuse shared-keys for message dispatch, where a potential enemy can dispatch a replay assault misusing the old key as the most current key is being engendered to each the hubs in the WSN.A time-exact counter might be embed to all bundle to check the cleanness of the parcel [6].

4.4 Self-organization

Each hub in a WSN must act naturally arranging and self-recovery. This nature of WSN additional poses makes great difficulties to wellbeing. The WSN dynamic nature makes it at times impractical to establishment any pre-introduced shared key system the few hubs and the BS. A number of key pre-dispersion frameworks have been characterize inside the setting of symmetric encryption However, for programming of open key cryptographic procedures a productive instrument for key conveyance could be exceptionally an incredible arrangement vital. It's ideal that the hubs in a WSN self-set up among themselves no longer easiest for multi-bounce directing however likewise to carryout scratch control and developing put stock in relations.

4.5 Authentication

The imparting hub is the one that it cases to be. A foe can't just change information bundles yet additionally can alter a parcel stream through embeddings manufactured parcels. It's, along these lines, essential for a collector to have a system to affirm which they got parcels have for sure touch base from the real sender hub.

5. PROPOSED WORK FOR SECURITY OF DATA IN WSNs

5.1 DES

DES is a symmetric algorithm that is uses in encryption of message as well as decryption of that message. DES calculation takes plaintext of fixed length and converts that plaintext into cipher text of same length and every block of text is 64 bits in length. In DES algorithm 16 stages of processing, that is called rounds and initial permutation and final permutation that named such as IP for initial permutation and FP for final permutation [5][20].

5.2 MD5 Algorithm

MD5 algorithm process is something like that in which takes input of random length but produce output 128 bit after digest the data. Message digest algorithm is mostly used algorithm in hash function. Message digest functions used to produce digital signature of data. Mathematical functions of MD5 algorithm is uses to create several message digest for every message [7]. MD5 algorithm involves the following steps of processing information.

1. Adding the padding bits
2. Adding the size of message
3. Starting of MD buffer
4. Development data blocks of 512 bit.
5. Output generation.

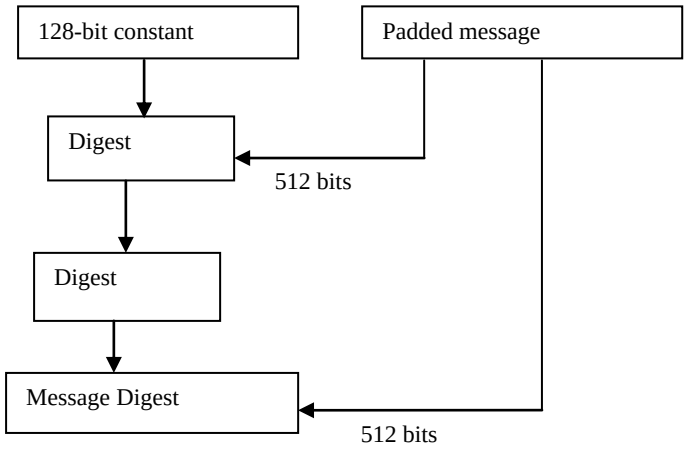

Fig 2: Structure of MD5 Algorithm

5.3 SHA-1 Algorithm

SHA-1 is the part of mostly used security algorithm and mechanism and protocol that is TLS and SSL. SHA-1 calculation is basically useful for protecting the long length message or information. SHA-1 algorithm has also used in digital signature for verification at the time of booting that doesn't allow the intruder to enter in the organization. In this calculation of information the algorithm takes the input of various sizes but gives the output of 160 bit in length after the digest of message. These are the steps of calculation over data.

1. Adding the padding bits
2. Adding the size of message
3. Produce processing function
4. Produce processing constant
5. Start Buffers
6. Development data blocks of 512 bit.

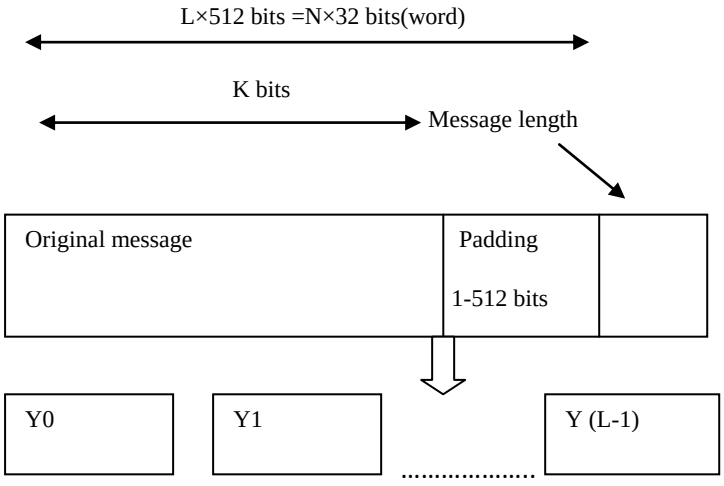

Fig 3: Structure of SHA-1 Algorithm

6. RESULTS

6.1 DES

In this section, implementing the result of DES algorithm by which could prevent the data when send from source to destination. Because according to the DES algorithm we are using secret key for encryption as well as for decryption of message.

Fig 4: Result of DES Algorithm

6.2 MD5 and SHA-1

In this section, shows implementation of MD5 and SHA-1 algorithms. These are the message digest algorithm which uses hash function at the time of calculation on the information. According to the algorithm here we are using the input string that will be digest by the MD5 or SHA-1 and gives specific output.

For the verification of processing data here using digital certificate by which we can check that information is reaching on the right place or not. By using digital signature could verify the information authentication.

Fig 4: Result of MD5 Algorithm

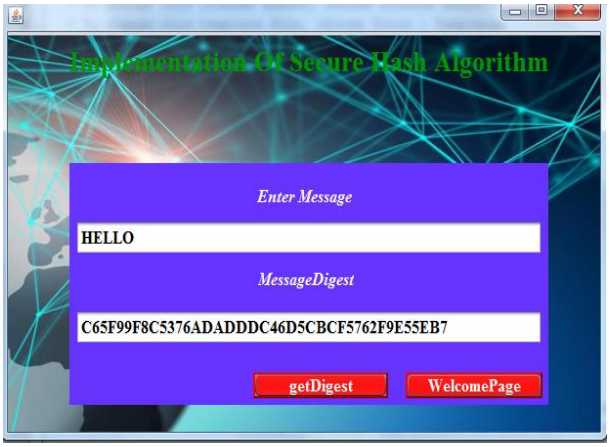

Fig 5: Result of SHA-1 Algorithm

In fig 5 and fig 6 shows the result of MD5 and SHA-1 algorithm by which data digest using the hash function and all

the information will be safe by using these algorithms. In fig 7 shows the verification of information that is authentic or not.

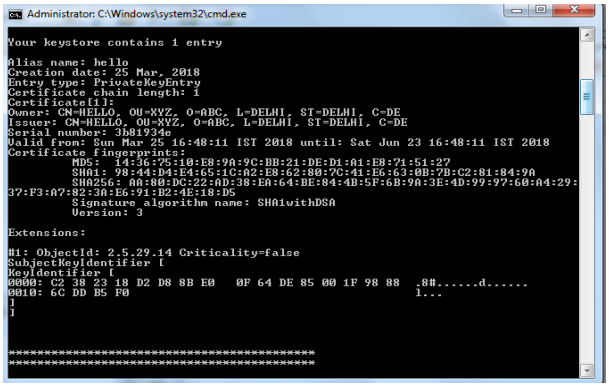

Fig 6: Verification of data

Table 1: Comparison of Hash function and symmetric algorithm

Feature/ Algorithm	Hash	Symmetric
No of Keys	0	1
key length	256 bits	128bits
Sharing effect of key	N/A	Big Issues
Speed	Fast	Medium
Complexity	Less	High

7. CONCLUSION

In this paper we have discuss on the MD5 and SHA-1 algorithm over DES algorithm. For the security of data needs some logic otherwise intruder can harm the system. Here comparing the DES algorithm with MD5 and SHA-1 algorithm on the basis of speed and complexity of algorithms, by which find that SHA-1 algorithm is much better than DES algorithm because SHA-1 algorithm takes less time and complexity of this algorithm is less, here we are using SHA-1 algorithm in wireless sensor network than can save the time as well as energy of the sensors. In future work we can reduce the energy consumption of sensor in wireless sensor networks.

8. REFERENCES

[1] T.-H. Lin, C.-Y. Lin, and T. Hwang, ―Manin-the-Middle Attack on ‗Quantum Dialogu with Authentication Based on Bell States‘, International Journal of Theoretical Physics, pp. 1–5,2013.

[2] Z. Tan, P. Nanda, R. P. Liu, A. Jamdagni, and X. He, ―A System for Denial-of-Service. Attack Detection Based on Multivariate Correlation Analysis,‖ IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. 1, p. 1, 2013.

[3] U. Banerjee, A. Vashishtha, and M. Saxena, ―Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection, International Journal of Computer Applications, vol. 6, no. 7,pp. 1 5, Sep. 2010

[4] Dr.Asir Antony Gnaana Singh, E.Jebamalar Leavline‖ Data Mining in Network Security - Techniques & Tools: A Research Perspective‖, Journal of Theoretical and Applied Information Technology 20 November 2013. Vol.57 No.2.

[5] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.

[6] Pranab Garg1, Jaswinder Singh Dilawari2, A Review Paper on Cryptography and Significance of Key Length, IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012.

[7] Vishwa gupta,2. Gajendra Singh ,3.Ravindra Gupta, Advance cryptography algorithm for improving data security, www.ijarcsse.com, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[8] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, www.ijarcsse.com, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[9] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518.

[10] Debasis Das1, U. A. Lanjewar2 and S. J. Sharma3, The Art of Cryptology: From Ancient Number System to Strange Number System, Web Site: www.ijaiem.org, Volume 2, Issue 4, April 2013 ISSN 2319 – 4847.

[11] E. Thambiraja, G.Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques," International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[12] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

[13] Vikash Kumar, Anshu Jain,P N Barwal " Wireless Sensor Networks: Security Issues, Challenges and Solutions "International Journal of Information & Computation Technology, Vol. 4, Number 8 (2014), pp. 859-868.

[14] Raja Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi "Security Issues and Attacks in Wireless Sensor Network"World Applied Sciences Journal 30 (10): 1224-1227, 2014.

[15] Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani " Routing Attacks in Wireless Sensor Networks:A Survey,International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.

[16] K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi "Various Attacks in Wireless Sensor Network:Survey" International Journal of Soft Computing and Engineering, Vol.3,Issue-1, March 2013.

[17] Gursewak Singh, Rajni Bedi," A Survey of Various Attacks and Their Security Mechanisms in Wireless Sensor Network", International Journal of Emerging Science and Engineering (IJESE), Volume-2, Issue-8, June 2014.

[18] Dr. Banta Singh Jangra, Vijeta Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and

Innovative Technology (IJEIT) Volume 2, Issue 3, Sep 2012.

[19] C K Marigowda1, Manjunath Shingadi, "Security Vulnerability Issues In Wireless Sensor Networks: A Short Survey", International Journal of Advanced Research in Computer and Communication Engineering,Vol.2, Issue 7, July2013.

[20] Prerna Mahajan & Abhishek Sachdeva,"A study of Encryption Algorithms AES, DES and RSA for Security", Global journal of Computer Science and Technology, Vol.8,No.15, (2013) pp.15-22.

[21]