ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Analysis of Various Authentication Algorithms in Wireless Sensor Networks

Anupama Khatak
M. Tech Student
Department of Computer Engineering
Punjabi University, Patiala, Punjab, India

Raman Maini
Professor
Department of Computer Engineering
Punjabi University, Patiala, Punjab, India

Abstract: With the passing challenging years there is an advancement in technology from wireless communication networks to wireless sensor networks. These sensor nodes are capable of exchanging information using radio singles. Collection of hundreds of thousands of such sensor nodes are typically defined as wireless sensor networks. Wireless sensor nodes are placed unattended, in open social environment to monitor environmental and physical conditions. They are adaptable to maintain vast range of functions. In this work various attacks, authentication algorithms, and their comparison has been discussed. It has been observed that RSA algorithm reside on the key size and the significance of the exponent, ECC resides on the key size and the type of algorithm. whereas hash, due to its compressed output it computes fast operations.

Keyword: Index terms- WSN, sensors, networks, nodes, attacks, authentication, algorithms.

1. INTRODUCTION

In the world of computer networks to recount telecommunication, wireless term is used in which electromagnetic waves are used to carry the singles and maintain communication. Wireless networking demands NICs, APs and routers instead of wire. A device that identify and react to some kind of data from the physical domain are the sensors. In sensors, data could be motion, pressure, temperature and output is generally a indicator that is connected to human readable form. Network is a collection of two or more computer system that are connected together to exchange data , share common resources.[1]

Summing up of all the above terminologies makes wireless sensor network. The network that's formed by a huge count of sensor nodes where every node is arranged with a sensor in it to identify physical phenomena such as light, heat, pressure, etc. [1]This paper summarize the basics related to the wireless sensor networks, attacks, algorithms and its advantage to the environment or to the humans.

In the section 2 wireless sensor networks are explained along with standards and characteristics.

Section 3 comprises attacks being faced. Further sections includes algorithms related to authentication and thus their exciting comparison.

2. WIRELESS SENSOR NETWORK

Wireless Sensor Network is basically a self-configured as well as infrastructure less networks for checking environmental conditions such as temperature, sound, motion, pressure etc.[1] It is used to canyon the facts to the sink for analysis and observations. A sink also called base station is an interface and using it any user can access required information from network. WSN works with the help of sensor node. Sensor nodes have a system of radio single which help sensor nodes to communicate. A wireless sensor node is furnished with sensing and computer devices, radio transceivers and power components.[4] Every node in WSN have their own characteristics such as activity fastness, storage accommodation and transmission bandwidth.[4]

A wireless sensor network has three segments: Sensors Nodes, Sink Node (User)[1] and Target Nod, as shown in Figure below.

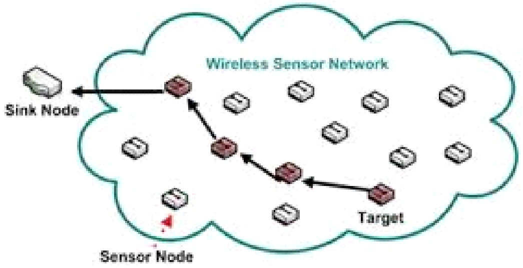

Fig: 1 Wireless Sensor Network [1]

When a particular sensor node is opened, it start to approach for the required information demanded by the user. 'control site' can also be used to send queries to wireless sensor devices. Sensor nodes may work continuously or as per wireless sensor devices can be forced to 'act' upon certain conditions;[4] thus the network are called 'Wireless Sensor and Actuator Networks'.[4]

3. ATTACKS IN WSN

- **Clone Attacks** are the node attacks. In this attack the manager of the node audit the link channels and destroy the confidentiality of the information. It is an adversary in the form of a person or another entity that poses a threat to the secrecy of data, replicates the captured nodes and arrange these random replicas throughout the network. In this attack cryptographic information is copied from sensor nodes to the other node known as cloned node. It is considered as honest node by its neighbors as honest node are unaware of the presence of clone among themselves.[7]

- **Man in the Middle Attack** is a form of attack that traces the private conversation of victims and add new information into their personal talk. This is done by establishing sovereign pairing with the fatality and transferring informationamong them, ensuring them that they are exchanging message over a separate network.[7]

- **Sink Hole Attack** is a type of attack in which compromised node is used to route the data from surrounding nodes by forging routing information into it and making it more attractive. This will make easy flow of all the jam from huge field in the system through opposers node to simplify selective forwarding. [7]
- **Jamming**is a kind of attack on the physical layer of wireless network which interrupts the radio frequencies used by the network nodes. An impressive network which uses simple frequency can be halted by jamming and it also surges the energy consumption of a node by injecting irrelevant packets. This further effects the receivers nodes as it will consume higher energy because of those packets.[7]
- **Flooding** in this attack, network performance is distributed greatly by generating large volume of traffic to prevent the user from accessing services and blocking either the node or link along with the node in flooding. Buffer/storage of target node gets overflowed because of the multipleconnection requests triggered towards the target node, making it unable to handle. Thus, the node becomes incapable to provide any further services to the clients.[7]

4. AUTHENTICATION ALGORITHMS

Wireless sensor nodes are placed unattended, in open social environment to monitor environmental and physical conditions. Due to this reason WSN are easily vulnerable to attacks. Thus, to maintain secure communication, authentication of network is required. Following are the authentication algorithms for wireless sensor networks.[5]

4.1. RSA ALGORITHM

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman who discussed the algorithm in 1977. This method is used to encrypt the message without requiring the secret key separately.[8][9]Step generation are as follows:

1. Choose two different prime numbers, r and s.[8][16]
2. Compute **n=rs** [8][16]
3. Compute phi or select the public key E,[8] such that it is not a factor of (r-1) and (s-1) [16]
4. Compute the private key D, such the equation comes to be true **(D*E) mod (r-1)*(s-1)=1**[16]
5. Calculate the cipher text CT from the Plain text PT, **$CT=PT^E$ (mod n)**[16] for encryption. [16]
6. Send the cipher text to the receiver.[8][9]
7. Calculate the plain text PT from cipher text CT, **$PT=CT^D$ (mod n)**[17] for decryption.

PARAMETER OF RSA :

1. Key size- It uses large key prime numbers.[8]
2. Memory- high memory usage.[8]

4.2. ECC ALGORITHM [2]

ECC stands for Elliptic Curve Cryptography. It is founded by Victor Miller and Nil Koblits in 1985.[8] It is the another method for executing public key cryptography. Equation for ECC is **$y^2=x^3+ax+b$**. [8]

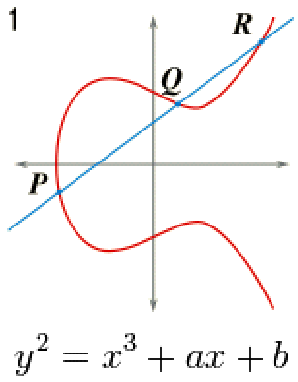

Fig-2 Elliptic Curve [8]

Key generation : here, we generate the public key (Q) and the private key (d).[6]
To generate the public key we use the equation : **Q=d*P** ,[8]
where d= any number selected within the range of (1 to n-1).
P is the point on the curve.[8]
n is the maximum limit (always a prime number).
PARAMETERS OF ECC:

1. Key size- It uses small key size.[8][6]
2. Memory- low memory usage.[6][8]
3. Transmission- low transmission requirements.[8]

4.3. HASH ALGORITHM

A hash algorithm is defined as a function that transform the data numeric value into a string of fixed length. Algorithm consists of rounds of hash function. Every round receives the input combination of recent messages block and output of the last round. Such procedure is processed as many times as required to hash the complete message. Hashes are widely used to notice if any changes are performed in data objects.[3][12]

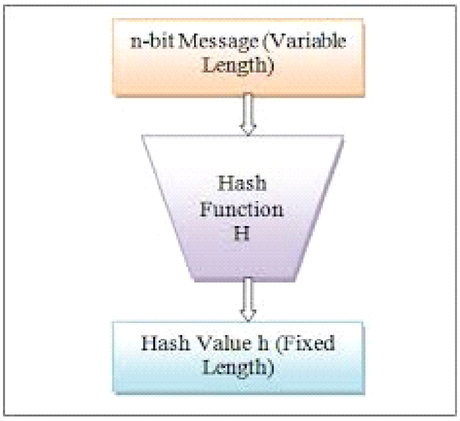

Fig-3 Hash Function [3]

Typical hash algorithms include MD5, SHA-1, and SHA-256.[10]

4.3.1 **MD5**

MD stands for Message Digest. Here, we will discuss MD5 hash algorithm as is widely used.

- It incorporate the one-way hash function for the conversion of messages, providing affirmation related to the integrity of transferred file.
- It make use of 128-bit hash function[10].
- Because of the transformation nature, original message is infeasible to calculate from the message digest.

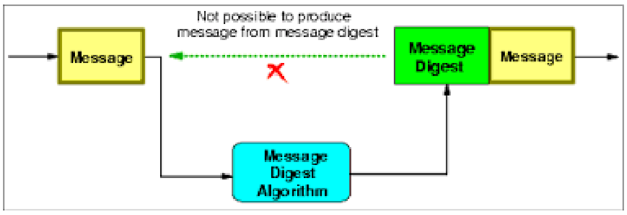

Fig-4 Message Digest [10]

- It can be used with authentication header (AH), internet key exchange (IKE).
- It is no longer in use, because collision were found in 2004.[12]

4.3.2 **SHA-1**

SHA stands for Secure Hash Function. Most used hash function is SHA-1.

- It is known as the strongest algorithm than MD5.[3]
- It make use of input of 264-bit in length and provide 160-bit message digest.[10]
- It can be used with AH, encapsulating security payload (ESP), IKE.
- SHA-256 is a variation of SHA-1.[12]
- Due to uncovered collisions, SHA-1 remains doubtful in 2005.

5. ANALYSIS OF DIFFERENT AUTHENTICATION ALGORITHMS

RSA algorithm encryption is used for long messages without embedding the symmetric encryption, due to this reason it provides highest security in the business applications.Advantages of RSA algorithm is that it uses public key encryption also it can be used to sign a message. But when it comes to factorization of large prime numbers the method faces difficulties. RSA need's high memory storage to store these large numbers, which is considered actually an issue.[11]
ECC algorithmsare used for small key size messages, hence it gives a magnetize security solution for wireless networks. It provide same level of security as that of RSA with larger key, eg; 256-bit ECC public key is providing comparable 3072-bit RSA public key. Advantage of ECC is that it is considered as the best security solution as it favors low memory usage. The problem faced by ECC is the size of elliptic curve.[12]
Hash algorithms involve hash function which are highly involved in the security issues. Hash generate out the smaller value than its input value that is between 160 and 512 bits. It computes a fast operation than the symmetric encryption because of its compressed output nature. Data integrity check and password storage is the most common application of hash functions.[13]
However, we concluded that both RSA and ECC are public key cryptosystems whereas, hash function concentrate much on the length of the hash value. Since, all three of them provide security to the applications but hash function has had area of interest in the past decades as compared to ECC and RSA.[14]
Since, ECC uses small messages to be computed memory required to store the data is less as compared to the RSA algorithm which is meant for the large number factorizations but due to the size of elliptic curve ECC too lack interests in the field.[15] In case of size of encrypted data files RSA shows 64-512 byte and ECC shows 73-595 byte respectively. Hash function involves rounds which are quite different from both RSA and ECC algorithms.

6. CONCLUSION

This paper discuss various fundamental certainty's associated with wireless sensor networks, its benefits to the society and environment. It involves the number of attack that take place to capture the information of the network, hence destroying the confidentiality and disturbs the authentication of the network. Since, authentication is the verification of the sender's uniqueness, one must be very careful. Here, we have mentioned various authentication algorithms of WSN along with algorithms, their comparative analyses. It has been concluded that hash function are used to specify the changes performed by the data objects, to attain a provided security level a smaller key size is required in case of ECC than in RSA, i.e; " security-per-key-bit" rate is higher. Since ECC consist of difficult mathematical background our future work will concentrate on RSA factorization problem to promote score itemized result.

REFERENCES

1. https://www.intechopen.com/books/wireless-sensor-networks-technology-and-protocols/overview-of-wireless-sensor-network
2. https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/
3. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
4. https://en.wikipedia.org/wiki/Wireless_sensor_network
5. https://www.juniper.net/documentation/en_US/junos/topics/concept/ipsec-authentication- solutions.html
6. http://www.ijcsmc.com/docs/papers/June2013/V2I6201330.pdf
7. International Journal of Scientific & Engineering Research Volume 3, Issue 3, March-2012
8. http://edge.cs.drexel.edu/regli/Classes/CS680/Papers/EC_prezentacio.pdf
9. International Journal of Network Security, Vol.18, No.1, PP.82-89, Jan. 2016
10. Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 108-117, 2015 ISSN 1990-9233 © IDOSI Publications, 2015 DOI: 10.5829/idosi.mejsr.2015.23.ssps.30

11. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.
12. Ahmed Al-Riyami, Ning Zhang, and John Keane, "Impact of Hash Value Truncation on ID Anonymity in Wireless Sensor Networks," *Ad Hoc Networks*, Vol. 45, pp. 80-103, March 2016.
13. Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, and Qun Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks," *Journal of Sensors*, pp. 1-9, September 2016.
14. International Journal of Advanced Research in Computer Science and Software Engineering 4(7), July - 2014, pp. 236-23
15. Bara‟a A. Attea, EnanA.Khalil, "A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks" journal of Applied Soft Computing (2011).
16. M. Preetha et al, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 6, June- 2013, pg. 126-139