Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Network Security Described Technology Based on RSA and Biometrics for Authenticity in WSN

Sandhya Katiyar
Professor, In Department of Information & Technology, Galgotiya's College of Engineering and Technology, Greater Noida, India

Shumaila Rizwan*
Department of Information & Technology, Galgotiya's College of Engineering and Technology, Greater Noida, India

Dr. Rajnish Gujral
Professor, In Department of Computer Science & Engineering, M.M.U. Mullana, Ambala, India

Abstract-- Security in wireless sensor network (WSN)is concern for a sensor networks and level of security desired may differ according to application specific needs where sensor networks are deployed. Most of the security techniques are used in WSN. The sensor nodes (SN) is used to collecting the information from the environment so it is necessary to secure our environment. There are many types of security provide in the field of WSN. We are take two technologies RSA algorithm and Biometrics techniques for the authentication in WSN and they are very effective to securing the information and massege security by cryptographic technique and give the best result for authentication in WSN. These thechnologies are use to veryfing the conformation of every single sensor node.

Keywords-- WSN, Biometric, RSA, Security, Authenticatin, Cryptography.

I. INTRODUCTION

Wireless Sensor Network (WSN) is used for collecting the information from the environment. WSN consist of a large number of Sensor Nodes (SN). Each SN in the network are connected by a wireless channels.The node will sense the environmental data and send to the other sensor nodes or Base station. During the transmission of data from one node to another node, different security techniques are used. To implement security, such as confidentiality, integrity and authentication keys are needed.

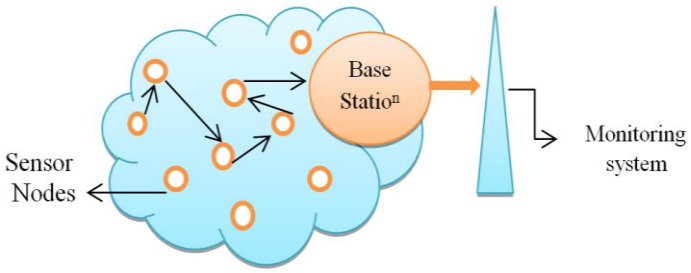

Fig1; Wireless Sensor Network Architecture

A sensor attached with the human body it periodically collects heartbeat temperature and transmits to the base station. The base station sends the information to the monitoring system. The information which is send to the base station should be protected this information transmitted securely [1]. Security issue in routing protocol have not given much attention, since most of the routing protocol in WSN_s have not beendeveloped with security in mind. Many hierarchical routing protocols have been developed, where energy efficiency is the main goal. In many application like military and battle field, data is important and have to maintain security in data communication between sensor nodes and BS.

Cryptographic data primitives are the basis of security solutions and the most frequently executed security operations in sensor networks. Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the study of hiding information that enables to store sensitive information and also transmit it across insecure networks but it cannot be read by anyone except the intended recipient. Symmetric algorithms, both parties share the same key for encryption and decryption. The most common types are;

(i) Symmetric key cryptography and

(ii) Public key cryptography.

A Public key cryptography algorithm uses two different keys for encryption and decryption [2]. The cryptography algorithm RSA is currently the most used among the asymmetric algorithms, working form the difficulty of factoring large numbers. This algorithm is widely used in transections on the Internet.

The security of biometrics in WSN such as Biometric authentication is the process of verifying if a user is whom he is claiming to be using digitized biological signatures of the user. This technique is also use for authentication security.

The rest of this paper is organized as follows: previous related work is discussed in section II. A detail of RSA algorithm and Biometrics features in discussed in section III. Comparing performance of RSA and Biometric in section IV and finally, the paper concluded in section V.

II. RELATED WORK

Solving the problem or wireless sensor network security is not an easy task. The source authentication protocols for WSN used for cryptographic techniques, which don't require computational and high communication overhead. Some of the authentication protocols in WSN µTESLA [3]. This protocol requires symmetric cryptographic techniques. One way hash chain is use for generating authentication keys. In µTESLA, it send the key chain commitments using unicast, it consist of starting time and duration of the time interval, but it is not applicable in large sensor networks, more DOS attacks in there then the authentication is delayed in µTESLA. To avoid this problem later multi-level µTESLA [4] was proposed. Multilevel key chain is applied in a large WSN. The higher level is used for authentication the lower level. The lower level is used to authenticate the message. Multilevel chain is use for increasing the lifetime. The limitation of this scheme is to suffer from authentication delay.

Many security protocols were proposed trying to efficient carry out the problem of security and the constraints of wireless network [5]. The strong cryptography algorithm, such as RSA algorithm is proposed to be used in WSN_s even there a lot of constrains including high time complexity and power consumption. The RSA coding algorithm are outline the four processes needed for RSA encryption, i.e.

a. Creating public key
b. Creating a private (secret) key
c. Encryption messages
d. Decoding messages

In brief, the RSA algorithm is following [6]:

To create public key Kp:

a. Select two different primes P and Q
b. Assign x=(P-1)(Q-1)
c. Choose E relative primes to x, which must satisfy a condition for Ks.
d. Assign N=P*Q
e. KPis N concatenated with E.

To create the private key:

a. Choose D:D*E mod x=1
b. Ks is N concatenated with D.

To encode plain text m by:

a. Assume m is a numeric
b. Calculate $c= m^E \bmod N$.

To decode c back to m

a. Calculate $m= c^D \bmod N$.

Elliptic curve cryptography (ECC) [7] has been proposed for public key cryptography (PKC) for solving the problem of authentication in WSN. ECC based schemes and identity (ID) based schemes have high energy consumption. The ID based signatures require that pairing or well paring. Computation which leads to a high computation cost and energy consumption is high. The communication cost is high due to the size of the signature. The signature based schemes gave been proposed for resource constrained networks.

The Biometrics authentication in WSN establishment is very useful technology to providing the security, in 2010 Yuan et al. [8] proposed the first biometric-based user authentication scheme for WSN_s. their scheme is very efficient since only the hash function is used in it. However, Yoon et al. [9] pointed out that Yuan et al.'s scheme is vulnerable to the insider attack, user impersonations attack, GW-node (gateway node) impersonation attack and sensor node impersonate attack. To improve security, Yoon et al.'s proposed an improved scheme and claimed their scheme could withstand various attacks.

Many of the existing works onthese techniques for WSN authentication security, the difference in my work is that it focuses on the techniques of security and performance in RSA and biometric.

III. TECHNIQUES FOR THE WSN SECURITY

There are so many techniques are used for security in WSN but, we are discuss about the two techniques that is RSA algorithm and Biometric techniques for authentication purpose,

A. RSA (Rivest-Shamir-Adleman)

A cryptographic algorithm is mainly used-RSA. By using this, the data packets are transferred through dynamic routing by time to time key value change securely. RSA implements two important ideas, Public – key encryption and Private – key decryption. In RSA encryption key are public, while the decryption key are not. The person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. Through this process the lifetime of sensor node is increased.

i. RSA work and Use [10].

- Each user generates public/private key pair by:
  1) Selecting two large primes at random p, q (secret)
  2) Computing their system modules N= p. q (public)
  Note $\phi(N)=(p-1)(q-1)$ (secret)
  3) Selecting at random the encryption key e (public)
  Where $1<e<\phi(N)$, GCD $(e, \phi(N)) = 1$
  4) Solve following equation to find decryption key d (secret)
  e. d =1 mod $\phi(N)$ and 0=d=N
  Use the extended Euclid's algorithm to find the multiplicative inverse of e (mod ϕ (N))
- Publish their public encryption key: KU = {e , N}
- Keep secret private decryption key: KR = {d , p , q}
- Each block is represented s an integer number
- The block size is <= $\log_2(N)$ bits
- If the block size is k bits then
- 2k<= N <= 2k+1
- To encrypt a message M the sender:
- Obtains public key of recipient KU = {e , N}
- Computes: C=M. e mod N,
  Where 0=M<N
- To decrypt the cipher text C the owner:
- Uses their private key KR = {d , p , q}
- Computes: M=Cd mod N
  Note that the message M must be smaller than the modulus N (block of needed) because of Euler's Theorem:a ϕ (n) mod N = 1
  Where gcd (a, N) = 1
- In RSA have: N = p. q
- $\phi(n)= (p-1) (q-1)$
- Carefully chosen e & d to be inverses mod $\phi(N)$
  Hence e. d =1+k. $\phi(N)$ for some k
- Two cases:
  1) gcd (M, N) = 1
  2) gcd (M, N) > 1

ii. RSA Algorithm Example

- Choose p=3 and q=11
- Compute n = p*q = 3*11 = 33
- Compute f (n) = (p-1)*(q-1) = 2*10 = 20
- Choose "e" such that 1< e < f (n) and "e" and "n" are co-prime. Let e = 7
- Compute the value for "d" such that (d*e)%f(n) = 1
  On solution is d = 3 [(3*7) % 20 = 1]
- Public key is (e, n) => (7,33)
- Private keys is (d, n) => (3, 33)
- The encryption of m = 2 is c = 27 % 33 = 29
- The decryption of c = 29 is m = 293 % 33 = 2

Cryptography is basically the conversion of data into a secret code for transmission over a public network. Today's cryptography is more than encryption and decryption. Cryptography is the study of mathematical systems for solving two kinds of security problems: privacy and authentication, and these encryption and decryption methods are using in the WSN for authentication security provides the sensor environments to be secure the transmission of information.

B. Biometric security features

Biometric keys are proposed which is measurement of physiological or behavioural features that identify a person (authentication by something inherent). Biometrics measures features that cannot be guessed easily.

i. Components

Several components are needed for biometric, including capturing devices, processors and storage devices.

- 'Capturing devices' such as readers (or sensors) measure biometric features.
- 'Processors' change the measured features to the type of data appropriate for saving.
- 'Storage devices' save the result of processing for authentication.

ii. Enrolment

Before using any biometric technique for authentication the corresponding features of each person in the community should be available in the data base. This is referred to as enrolment.

iii. Authentication

Authentication is done by verification and identification.

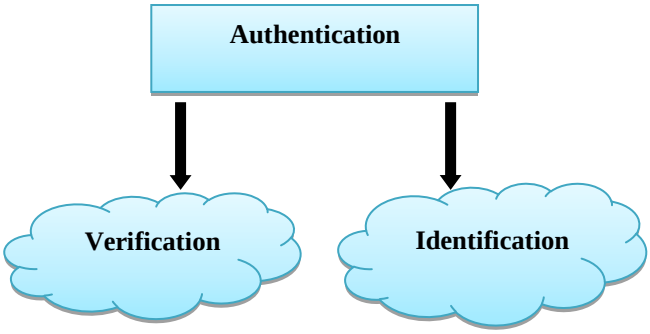

Fig2; Authentication Categories

- Verification, a person's feature is matched against a single record in the database (one-to-one matching) to find if she is who she is claiming to be. This is useful, for example, when a bank-needs to verify a customer's signature on a check.
- Identification, a person's features is against all records in the database (one-to-many matching) to find if she has a record in the database. That is useful, for example, when a company-needs to allow access to the building only to employees.

C. Biometrics Techniques

Biometrics techniques are divided into two broad categories:

1. *Physiological*

Physiological techniques measure the physical traits of the human body for verification and identification.

- *Fingerprinting*
  There are two most common are minutiae-based image-based method. In the minutiae-based technique the system creates a graph based on where individual ridges start/stop or branch. In the image based technique, the system creates an image of the fingertip and finds similarities to the image in the database.
- *Face*
  This technique analysed the geometry of the face based on the distance between facial features such as the nose, mouth, and eyes.
- *Iris*
  It measures the pattern with in the iris that is unique for each person. It normally requires the laser beam (infrared). They are very accurate and stable over a person's life. They also support the authentication.
- *Voice*
  Voice recognition measures pitch, cadence and tone in the voice. It can be use locally (micro-phone) or remotely (audio channels). This is mostly use for authentication. However, accuracy can be diminished by background noise, illness or age.

2. *Behavioural techniques*

- *Signature*
  In the past signature were used in the banking industry to verify the identity of the check writer. Signatures are mostly use for verification.
- *Key stroke*
  The key stroke (typing rhythm) technique measures the behaviour of a person related to working with a key board. It is not very accurate because the trait can change with time (people become faster or slower typists). It is also text dependent.

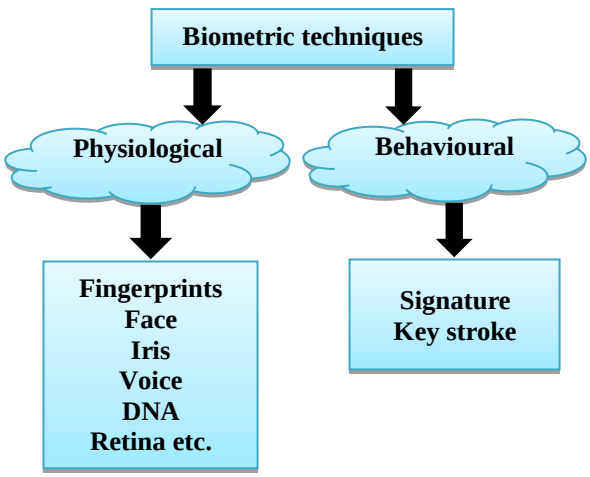

Fig3: Biometrics categories

IV. DESCRIBE THE RSA AND BIOMETRICS SECURITY REQUIREMENTS

The wireless sensor network security mechanisms require a certain amount of resources for the implementation such as: data memory, code space and energy to power the sensor.
These resources however are very limited in a tiny wireless sensor:

- Limited Memory and Storage Space.
- Power Limitation.
- Vulnerability of nodes to physical capture.
- Lack of a-priori knowledge of post-deployment configuration.
- Collision and latency.

Wireless sensor networks are vulnerable to many attacks because of broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environment. The security requirements of WSN_s are:

- *Authentication*
  Authentication techniques verify the identity of the participants in a communication. In sensor networks it is essential for each sensor node and the base station to have the ability to verify that the data received was really send by the trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. A false data can change the way a network could be predicted.
- *Confidentiality*
  Confidentiality is needed to ensure sensitive information is well protected and not revealed to unauthorized third parties. Confidentiality is required in sensor network to protect information traveling between the sensor nodes of the network or between the sensors and base station otherwise it may result in eavesdropping on the communication.
- *Integrity*
  Lack of integrity may result in in accurate information. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of information to function for e.g. it is unacceptable to have improper information regarding the magnitude of the pollution that has occurred.

TABLE – 1 TABLE FOR RSA AND BIOMETRICS AUTHENTICATION SECURITY TECHNIQUES CHARACTERISTICS

Characteristics Technology	RSA based	Biometric based
Easy to operation	Simple	Simple
Hardware used	No need to extra hardware require a key only	No need to extra hardware
Initial cost	Moderate	High as it requires specialized hardware which is also difficult to install in normal system
Running cost	Expensive of key maintenance	Very expensive
Changed	Changed as requirement	Never changed
Attacks	Guessing by trial and error	False match
Theft	Difficult, only theft with special techniques	Safe, only templates can be stolen

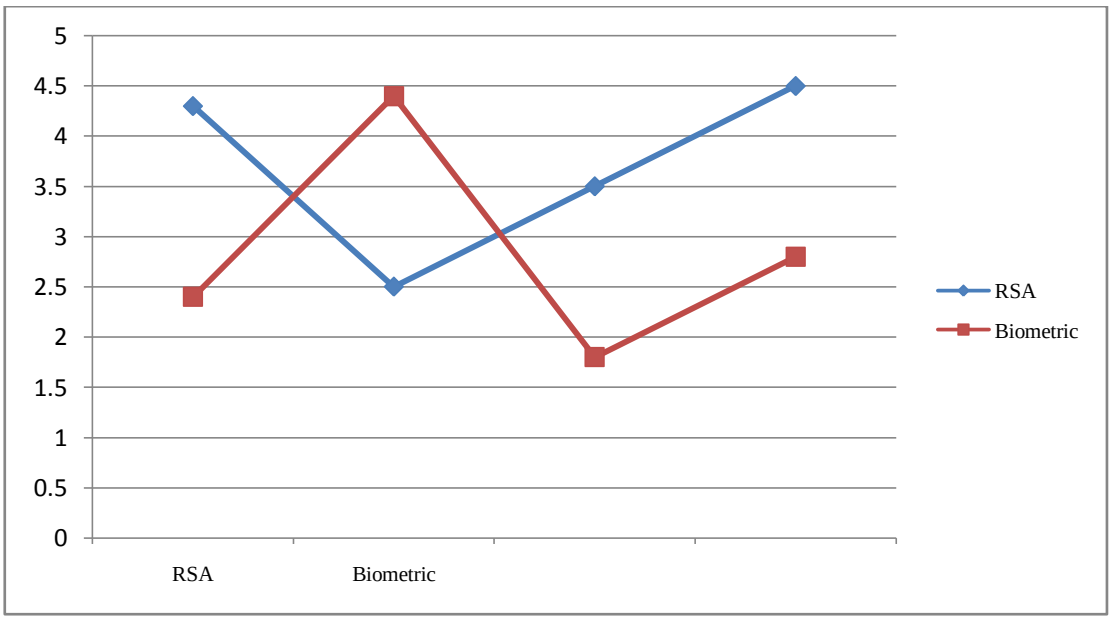

Fig4: performance of RSA and Biometric techniques

V. CONCLUSION

In the study of RSA algorithm and Biometrics techniques the main features that both are in cryptography based and using the purpose for authentication security. In wireless sensor network these technologies are secure and give the efficient results, sometime during the research RSA is better than Biometrics for cost and more reliable changing security keys and Biometrics is use for the hard and strong security. In the bases of performance and popularity they both are lightly similar, but they are useful in WSN authentication security.

REFERENCES

[1] L.Sujihelen, C.JayaKumar, "Authentication in wireless sensor network based on Virtual Certificate Authority" International Conference on circuits, power and computing technologies, 2013.

[2] Shanta Mandal and Rituparna Chaki. 2012. A Secure Encryption Logic for Communication in Wireless Sensor Networks. IJCIS. 2(3).

[3] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol", RSA CryptoBytes, vot. 5, 2002.

[4] Donggang Liu, Peng Ning, "Multilevel µTESLA: Broadcast authentication for distributed sensor networks", ACM Transactions on Embedded Computing Systems, Volume 3, Issue 4, pp: 800 -836, 2004.

[5] B. Kadri, A. Mhamed, and M. Feham "Secured Clustering Algorithm for Mobile Ad Hoc Networks", International Journal of Computer Science and Network Security, Vol.7, No.3, pp 27-34.2007.

[6] H. Anderson. Introduction to Computer Security, Prentice Hall, 2004, pp: 85-86.

[7] F.Hess, "Efficient identity based signature schemes based on pairings", In Proc. SAC, St. John's, Newfoundland, Canada, August2002.

[8] Yuan J., Jiang C. Jiang Z., A biometric-based user authentication for wireless sensor networks, Wuhan University Journal of Natural Sciences, vol. 15, no. 3, pp. 272-276, 2010.

[9] Yoon E., Yoon K., A New Biometric-based User Authentication Scheme without using Password for Wireless Sensor Networks, 2011 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 279-284, 2011.

[10] RSA key management technique in wireless sensor network (ICETS'14) Volume 3, Special Issue 1, February 2014.

