International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.2, May 2012 – www.ijais.org

Multi Factor Authentication Protocols for a Secured Wsn

R.Jayamala
Asst.Professor,
Anna university of
Technolgy,Trichy.

V.Eswari
Final Year M.E.,CSE
Anna university of
Technolgy,Trichy
eshwarivenkatachalam@gmail.com

K.Marimuthu
Final Year M.E.,CSE
Karpagam university
Coimbatore
marimuthupacet@gmail.com

ABSTRACT
WSN is an embedded system with the network properties of self configuration, self healing, dynamic routing and multi hop communication and sensor nodes are scattered in sensor field. WSN is ubiquitous in nature but nodes have limited energy resources and memory constraints, the protocols designed for sensor networks should be energy efficient. Security access to the sensor networks is a critical part of the network administration; due to wide availability of services and high mobility of users the strongest authentication methods are needed and hence we propose four factor user authentication protocols for a secured network. This scheme is based on multi factor such as password, smart card and a user finger print, phone factor.

Keywords
Secured networks, password, authentication, smart card, user finger print, Phone Factor authentication.

1. INTRODUCTION
Sensor networks can be viewed as a distributed autonomous system for information gathering, performing data intensive tasks such as environmental monitoring. Seismic monitoring, terrain surveillance. Sensor is an electronic device receives and response to stimuli. Sensor is available to detect chemical, radiation levels, lights, seismic activity, motion, audio and video. The elements of sensor nodes are sink, sensors. Sink will send queries and collects data from sensors will monitor phenomenon and report to sink.WSN is an embedded system having the properties of self configuration, self healing, dynamic routing, multi hop communication; self configuration is the formation of networks without any human interaction. self healing is the automatic deletion/addition of nodes without resetting the entire network.

Dynamic routing is the adaptive routing schemes on the fly based on the network conditions like line link quality, hop count, gradient ,etc. multi hop communication is used to improving the scalability and the network by sending messages peer to peer to a base station. Unattended ground sensor nodes are used by military to detect, classify, and track wheeled and tracked vehicles as well as personnel and possible threat. These sensor nodes can be deployed in environments that are not accessible or dangerous for men to enter.The technical challenges of adhoc deployment are that the system should identify and copes with the resulting distribution and connecting of nodes. Dynamic environmental conditions requiring the system to adapt over time to changing connectivity and system stimuli. Unattended operations require configuration and reconfiguration should be automatic (self configuration).

Security Requirements in WSN: Wide availability of services and the high mobility of users among different environments required the provision of security mechanisms to ensure the safe usage of services by legitimate users and the protection of services from unauthorized users because of wide range of services many diverse and flexible security models and mechanisms will be needed. Either standard security mechanisms will have to be embedded in the environment and used by all applications or each application will have to build its own security mechanisms.

Security has to be incorporated in the design stage. Traditional authentication and access control paradigms cannot scale to numerous and ubiquitous devices. Wireless communication is needed to enable mobility of communicating devices. Sensor nodes scattered in open areas can be compromised and used to carry out various attacks. Compromised node may cause collision with neighboring transmissions and leads to traffic monitoring activity to the internal wired attack. Attacks on WSNs can be classified as external wireless and internal wired attacks.External Wireless Attacks: An attacker uses a device to target the Access Point(AP) for accessing the network, Internal Wired Attacks: An attacker or an authorized insider inserts an unauthorized Access Point (AP) into the wired network for malicious activity. This can be detected by wireless traffic. Data volume is growing fast enough that it will force a change in the paradigm of cipher security. Security involves technical as well as social challenges.

2. RELATED WORKS
Over the decades, WSN's (wireless sensor network) security has got significant progress because sensor nodes are deployed in unattended environment. There is a strong need for providing security for accessing sensor nodes. In the recent decades many concepts which are providing security for wireless sensor networks are introduced. Here we relate some works which are based on user authentication protocols.

1. In 2001 M. Looi presented Enhanced Authentication Services for Internet Systems using Mobile Networks with the concept of adding additional factors to Internet user authentication significantly improves the strength of authentication.
2. In 2002 Taekyoung Kwon proposed a concept called Impersonation Attacks on Software-Only Two-Factor Authentication Schemes. However it can be vulnerable to impersonation attacks via interleaved sessions if a single server is compromised
3. In 2008 Manik Lal Das prposed Secure and Efficient Authentication Scheme for Remote systems which provides efficient mutual authentication scheme for remotesystems,
4. In 2009 M.L Das has proposed two factor user authentication for WSN which provides stronger user authentication, session key establishment and achieves efficiency.
5. .In 2009 Khan Algahathbar listed out some flows and vulnerability to various attacks in Das's scheme. He proposed improved version of Das's s scheme called

6.In 2010 Vaidya has pointed out that both Das's and Khan's Algahathbar's schemes are vulnerable to stolen smart card attacks and proposed improved two factor user authentication in WSN which provides robustness from various attacks. But this scheme also doesn't address session key establishment and mutual authentication between user and gateway node.
7. In 2010 Qiong Pu introduced An Improved Two-factor Authentication Protocol. He suggests key-compromise impersonation resilience should be added as one more important security requirement for two-factor based authentication scheme.
8. In 2010 Hui-Feng Huang and Ya-Fen Chang proposed Enhancement of Two-Factor User Authentication WSN.

Our protocol based on three factors such as password, smartcard and finger print. This provides robust security against above mentioned attacks and also provides session key establishment and mutual authentication.M.L Das proposed a two factor user authentication scheme which does not have active and passive attack. But Khan and Algahathbar pointed out that Das scheme does not provide mutual authentication . Here password cannot be changed and it has some flaws like bypassing attack and privileged-insider attack. So that we can store the authentication information in the smart card instead of gateway node since it is more secure. Even though the stealing of information from smart card is difficult and costly, there exist some attacks like invasive attack or side channel attack and stolen password attack.

3. THE PROPOSED SCHEME

This protocol is based on four factors such as password, smart card, phone factor and finger print. Password is a factor which you know and phone factor, smart card is a second factor something you have and biometrics like finger print is a third factor something you are.Username and password based authentication methods are known as knowledge based authenticator schemes which are most popular. Smart card, wipes phone factors based authentication methods are known as object based authenticator schemes. These are the physical devices so the user can carry. Biometrics like finger prints based authentication methods are known as ID based authenticator schemes. These factors provide strongest authentication mechanisms among other schemes. Each authentication schemes will have their own advantages and disadvantages. By combining the advantages of the above three methods we proposed an improved multifactor user authentication protocol which provides the robust security for WSN. Table I, shows a list of some notations and symbols will be used throughout the rest of paper.

TABLE-I

SYMBOL	DESCRIPTION
U_n	User n^{th} to login
S_n	Identity of sensors node
S_{node}	Sensor node
GWN	Gateway node of WSN
PWn	Password of U_n
ID_n	Login ID of U_n
FID_n	Fictitious ID of U_n
K	Secret key known to GWN only
X_n	Secret parameters generated by GWN and stored in designated S_{node}
H(.)	Cryptographic one way hash function.
‖	Bitwise concatenation manipulator
⊕	Exclusive –OR operator
=?	Verification operation
T_X	Concurrent time stamp, X=1,2,3
△T	Expected time interval for the transmission delay

In our scheme we consider the first two factors such as password and smartcard as like in previous scheme and we add another two factor called phone factor and biometrices (finger print) to meet all the security requirements of WSN.

3.1 Cryptanalysis Of Das's Scheme

A. Registration Phase

This phase is invoked when a user, Un, wants to register with the WSN. Un submits his/her identity (Sn) and password (PWn) to the GWN in a secure manner. Upon receiving the registration request, the GWN computes,

$S_{node} = h(ID_n \| PWn)$ XOR h(K),
where K is a symmetric key known to only GWN, Then the GWN personalizes a smart card with the parameters h(・), IDn, Snode, h(PWn) and Xn, where h(・) is a cryptographically secure hash function. Here, Xn is a secret parameter generated securely by the GWN and stored in some designated sensor nodes before deploying the nodes in the field, who are responsible to exchange data with users(We assume that a node is responsible for many applications. If the WSN is built for only one application then this secret parameter is known to all nodes). The GWN now send the personalized smart card to U_n in a secure manner. We note that X_n is not known to the user, as it is generated and stored in user's smart card securely by the GWN.
B. Authentication Phase The authentication phase is invoked when Un wants to perform some query to or access data from the network. The phase is further divided into Login and Verification phases.

1) Login Phase: Un inserts her/his smart card to a terminal, and keys ID_n and PW_n. The smart card validates ID_n and PW_n with the stored ones in it. If the entered ID_n and PW_n are correct, the smart card performs the following operations:
Step-LP1) Compute $FID_n = h(ID_n \| PW_n)$ XOR $h(Xn \| T)$, where T is the current timestamp of Un's system.
Step-LP2) Compute $Cn = h(Nn \| Xn \| T)$. Then send <FIDn, Cn, T > to the GWN.
2) Verification Phase: Upon receiving the login request< DID_n, C_n, T > at time T', the GWN authenticates Un by the following steps:
Step-VP 1) Validate T. If $(T' - T) \leq \Delta T$ then the GWN proceeds to next step, else abort, where ΔT denotes the expected time interval for the transmission delay.
Step-VP 2) Compute $h(ID_n \| PW_n)^* = DIDn$ XOR $h(X_n \| T)$ and
$Ci^* = h((h(IDi \| PWi)^*$XOR h(K)) $\| xa \| T)$.
Step-VP 3) If $C_n^* = C_n$, the GWN accepts the login request; else rejects it.
Step-VP 4) GWN now sends a message < DID_n,A_n, T ' > to some nearest sensor node, say, S_n, over a public channel to respond the query/data what Un is looking for, where

An = h(DID_n‖ S_n ‖X_a‖T'), and T' is the current timestamp of GWN system. Here, A_n is used to ensure the sensor node that the message < DID_n,A_n, T '> has come from the legitimate GWN, as A_n is generated with secret parameter X_n which is known to both sensor and GWN.

Step-VP 5) S_n first validates T' in similar line of **Step-VP 1**. Then S_n computes h(DIDn‖ Sn ‖X_n‖T') and checks whether it is equal to A_n. If these two checks pass correctly then S_n responds to U_n's query.

C. Password-Change Phase (PP) The password change phase is invoked whenever user U_n wants to change or update his/her old password (PW_n) to a new password, say PW_n*. The password change phase is described in the following:

1). User U_n inserts his/her smart card into the terminal and enters his/her identity (ID_n) and password (PW_n).

2). Now the smart card validates the U_n's entered ID_n and PW_n with stored values and check: if holds then the smart card request to the user for new password (i.e., PW_n*). Otherwise, rejects the password change request and terminates the operation.

3). Now upon receiving the U_n new password (PW_n*), smart card computes:

S_{node} *= S_{node} XOR h(ID_n||h(PW_n)||h(X_n)) =h(ID_n||h(PW_n *)||h(X_n)), here S_{node} is old stored value of the smart card (i.e., S_{node} = h(ID_n||h(PW_n)||h(X_n))).

4). Now the smart card replaces the old values (S_{node} and h(PWn)) with new values (S_{node} * and h(PWn *)). After performing the above steps, password change phase successfully takes places.

3.2 Token Less Approach

Phone factor is a token less approach which does not need a new password should be entered every time the user wants to access the network and also it should not need any token. It uses internet for user to access the sensor network and PSTN for the back end system to generate a call for the registered user's mobile phone. This scheme utilizes service management architecture to place a generated call from the internet to the PSTN.If a user wants to access the WSN then he must enter a username and password then the back end of the phone factor system rings a call to user's mobile phone then user have to accept the call with the password. If the above process is succeeded then the user is given access to the WSN.

This is an authenticated way because any intruder wants to access a remote node then it will be with the acceptance of authorized user only. Furthermore if the mobile phone is lost then the intruder should know the pin number of the mobile phone for accepting the call. If its pin number also compromised the above security mechanism is no longer worth.

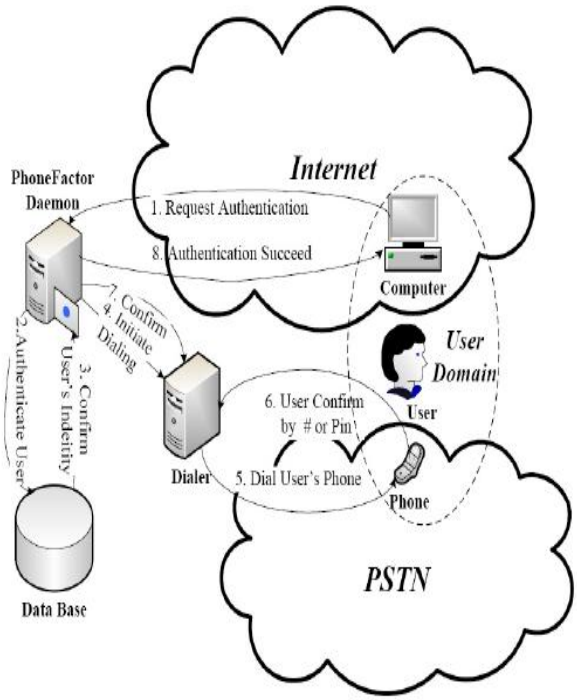

Fig 1. Phone Factor Authentication Systems

3.3 Palm print Authentication System (Finger print)

Biometrics is the study of automated method for recognizing a person based on his/her physical or behavioral characteristic. Biometric system has been actively emerging in various industries for the past few years, and it is provide higher security for access control system. Various technologies have been proposed and implemented including iris, fingerprint, hand geometry, face, and etc. identification technologies. Fingerprint and hand geometry is the most widespread biometric system in the world. However, fingerprint suffers from major drawback which is its proneness to anti-security threats, like the reproduction of fingerprints left on surface to deceive system. The hand geometry features are not descriptive enough for identification when the number of users grows larger. To overcome these problems zhang and shu proposed the new hand based biometric method called as Palmprint.

Palm has unique distinguishing line patterns which can be used to identify people uniquely. Palmprint not only has the information available on the fingerprint but it has far more amount of details in terms of principal lines, wrinkles, and creases. Palmprint is a combination of two unique features, namely, the palmar friction ridges and the palmar flexion creases (see Fig. 2). Palmprint Identification is an effective biometric technology that is gaining widespread acceptance and interest from researchers all over the world. There are some reasons which caused Palmprint identification find popularity (i) Low complexity, (ii) High accuracy (iii) Low resolution imaging, (iv) Stable line features, (v) High user acceptance.

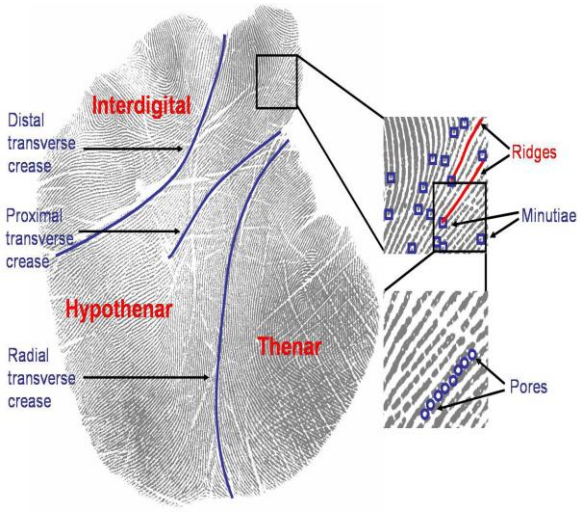

Fig.2. Regions, major creases, ridges, minutiae and pores in a Palm print

3.3.1 Image Preprocessing

Preprocessing is used to align different palmprint images and to segment the central parts for feature extraction. Most of the preprocessing algorithms employ the key points between fingers to set up a coordinate system. Preprocessing involves generally five common steps (Fig 3)

(1) Binarizing the palm images

(2) Extracting the contour of palms

(3) Detecting the key points

(4) Establishing a coordination system and

(5) Extracting the central parts.

Step1: The given image is converted to a binary image map according to the computed threshold value.

Step 2: The binary image is then passed through a filter and morphological thinning to produce the extracted edge image.

Step 3: The key points are identified according to the positioning of the two end points of the baseline from the palm print image.

Step 4: Construct a line through the two key points identified through the earlier step to retrieve the Y-axis of the coordinate system, and then a second line is drawn across the midpoint of the two key points which is perpendicular to the Y-axis, to determine origin of the coordinate system.

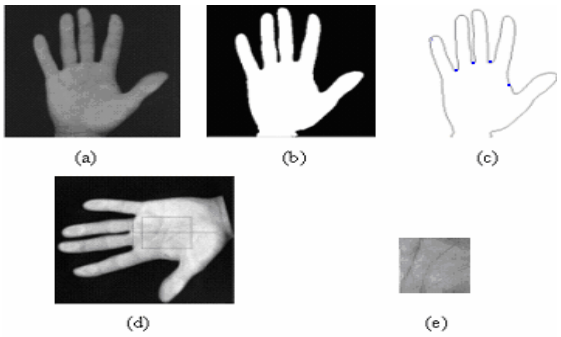

Figure (3(a-e)): The preprocessing steps

4. ANALYSIS OF MULTI FACTOR

We consider the first two factors password and smartcard as like in previous schemes and we add a phone factors as a third factor and finger print authentication as fourth factor to meet all security requirements of WSN.

A .Security Analysis of Multifactor

We present our proposed Multifactor schemes strength in terms of security analysis. Thus our proposed implementations schemes is phone factor and finger print authentication systems. In that scheme will shows the proposed frame work that resists against the following attacks.

1. Dos: Transport layer is needed when the system is planned to be accessed through internet or other external networks. The transport layer is vulnerable to DOS attacks. This vulnerability leads to connection with unsecured nodes.

2. Privacy Attacks: It is an attack for obtaining secret information .Bt notifying traffic in the network an attack will know about of different nodes, making it possible to find some events which he wants. Attackers can also insert a new node or compromise an existing node to behave like normal node for accessing secret information.

3. Replay Attack: An adversary can replay a previously extend huge without the knowledge of any keys. The adversary will buffer the encrypted and MAC protected manages and transmits it whenever necessary.

4. Sybil Attack: Single node presents many identities to the network that is one node can be in multiple places.

5. Traffic Analysis Attack: By analyzing the traffic, the attacker can identify the base station and hence making it easier to attack. There is no need for knowing the contents of communication for doing this.

6. Battery Depletion Attack: It is an attack that is aimed at depleting a sensor node's battery. Because battery is the heart to the sensor nodes.

7. Impersonation Attack: Node will try to present itself as certain another node in the network.

8. Cryptography: There are two methods used in cryptography, symmetric key and asymmetric (public) key cryptography. In symmetric key cryptography both sender and receiver will use the same secret key for encryption as well as for decryption. The problem associated with this symmetric key in a secure manner. Asymmetric key cryptography is also known as a public key cryptography. Sender will have public key to encrypt his data and only the intended receiver will have the corresponding private by(secret key) for decrypt that data, characteristics of algorithm used in the public key.

Cryptography make secure that the private key cannot be deceived from the public key.

B Performance Analysis of Multifactor

Here we are examine performance and summarize the security functionality of our multifactor frame work and compare with M.L.DAS Two factor scheme. Table II shows the multifactor authentication is more secured than two factor authentication. It also provides secured password change phase, provides mutual authentication secured against node compromised attacks and secured against denial of service attacks.etc.,

TABLE-II

Security Features	Proposed Scheme	Existing System
Secured password change and update phase	Yes	No
Provides mutual authentication	Yes	No
Protection against password guessing attack	Yes	Partial
Protection against attack with stolen smart card	Yes	No
Secured phone factor authentication	Yes	No
Secured Finger print identification	Yes	No
Security against node compromised attack	Yes	No
Security against denial-of-service	Yes	No
Computational cost for Registration and Login phase	3H	2H & 3H
Authentication/verification phase cost	7H	5H

5. CONCLUSION

In this paper, we have proposed an efficient multifactor user authentication protocol for wireless sensor networks. Which is imposed on four-factors (i.e., password, smart card, phone factor identification and palm print authentication systems) using cryptographic hash functions. We have provided security and performance analysis of the proposed schemes with existing frameworks. Furthermore, multifactor authentication provides more robust against various attacks like impersonation attack, stolen-verifier attack, password guessing attack, node-compromise attack, man-in-the-middle attack, denial-of-service attack etc., Palm print Identification plays an important role in personal identification Palm print identification is an effective technology to reduce the error rates and, improve the accuracy and high speed. So, here we conclude analysis of the proposed schemes provides more security and flexible than the other existing frameworks.

6. ACKNOWLEDGMENT

We here by thank Dr.R.Krishnamoorthy, Dean, Anna University of Technology Trichy for his moral motivation and guidelines for Multifactor Authentication protocol for a secured WSN.

7. REFERENCES

[1].Manik Lal Das, Member, IEEE Two-Factor User Authentication in Wireless Sensor Networks "IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS", VOL. 8, NO. 3, MARCH 2009

[2]. "An Improved Two-Factor Authentication Protocol 2010" Zhengzhou, He'nan, China Second International Conference on MultiMedia and Information Technology

[3]. Hui-Feng Huang and Ya-Fen Chang Chun-Hung Liu "Enhancement of Two-Factor User Authentication in Wireless Sensor Networks" 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

[4] E. H. (Jr) Callaway, Wireless Sensor Networks, Architectures and Protocols. Auerbach Publications, 2003.

[5] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," Wireless Networks, Vol. 8, No. 5, pp. 521-534, 2002.

[6] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in Proc. ACM Workshop Wireless Security, ACM Press, pp. 32-42, 2004.

[7] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proc. International Conf. Embedded Networked Sensor Syst., ACM Press, pp. 162-175, 2004.

[8] _ RSA SecureID, "Secure identity." [Online] Available: http://www.rsa.com/node.aspx?id=1156.