ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

Two Way User Authentication Using Biometric Based Scheme for Wireless Sensor Networks

Srikanth S P (Assistant professor, CSE Department, MVJCE, Bangalore)
Deepika S Haliyal (PG Student, CSE Department, MVJCE, Bangalore)

Abstract-Wireless Sensor networks (WSN) is excellent technology which provide great potential for situations like battlefields and commercial applications such as building, traffic survey, monitoring environments smart homes and many more scenarios. Security is the most important challenge in wireless sensor networks. Sensor networks does not have any user control for each individual node and wireless environment as they are typically deployed in an unattended environment, where the legitimate users can login to the network and access data as and when demanded. So as it is used for the critical purpose it is very important that only the legitimate users must be able to access that data and even if some intruder is capturing the information it must be in unreadable format. In this paper, we propose a new biometric-based user authentication mechanism in heterogeneous wireless sensor networks. The proposed protocol provides strong authentication compared to traditional related password-based schemes and achieves good properties like mutual authentication. Moreover, the project provides unconditional security against node capture attack and it is also resilient against different attacks.

***Index Terms*-Wireless sensor networks, authentication, wireless security, biometrics, hash function.**

I. INTRODUCTION

In a wireless sensor network (WSN), a large number of sensor nodes are deployed in a target field (also called a deployment field). After deployment of nodes, they form adhoc infrastructure-less wireless network. Nodes communicate with each other using wireless communication within their communication ranges and data are routed to the nearby base station(s) via multi-hop communication path. WSNs have numerous applications in field of military (for example, battlefield surveillance), hospitals and other real-time applications. Often WSNs are easy to deploy in a given area because nodes can be deployed randomly in the field and do not require constant maintenance. A large number of nodes could be dropped on a particular area from truck/plane and there after each node coordinates with their neighbouring nodes and together they form a network which is finally linked to a base station. Information gathered from the area of deployment is then passed on to the base station. In many sensor network applications, security and privacy of the collected data is a critical concern, since sensor nodes are usually deployed in insecure environments. In heterogeneous wireless sensor network there is a hierarchy among the nodes based on their capabilities: *base station, cluster heads and sensor nodes*. Sensor nodes are inexpensive, limited capabilities and generic wireless devices. Sensor node is equipped with limited battery power, memory size and data processing capability and short radio transmission range. Sensor nodes in a cluster/group communicate among each other in that cluster/group and finally communicate with the cluster head (CH)/ group head (GH). Group heads are more resource rich than traditional sensors. They are equipped with high power batteries, larger memory storage, and powerful antenna and data processing capabilities. Group heads can execute relatively complicated numerical operations than sensors and have much larger radio transmission range. Group heads can communicate with each other directly and relay data between its cluster members and the base station. A base station or gateway node (BS) is typically a gateway to another network, a powerful data processing/storage centre, or also an access point for human interface. In many security functions required in sensor networks, authentication is one of the essential requirements for secure communication. For authentication, digital certificates are known to provide the highest level of security, but since they are quite large in size and require public key signature verification, their usage in resource constrained environments is often limited. Biometric is considered as unique; care must be given in using the hash function. Here we have used SHA1 hash function which is well known for its one wellness and DES algorithm can be used for the symmetric encryption purposes. Traditional password-based authentication schemes [2], [3] are based on passwords and thus the security of these schemes is based on the passwords only. However, simple passwords are easy to break using simple dictionary attacks. Recently, biometric-based user authentication schemes [1] along with passwords have drawn considerable attention in research is a biometric-based scheme which is applied to the resource constrained WSNs. A biometric system is considered as a pattern recognition system such a system operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and then comparing this feature set against the template set in the database. Thus, the biometric verification allows one to confirm or establish an individual's identity. There are major advantages of using biometric keys (for example, fingerprints, faces, irises, hand geometry and palm-prints, etc.)

Threat to a Sensor Node:

Due to the hostile environments in the target field, nodes can be physically captured by an enemy. We assume that both the sensor nodes as well as group heads can be compromised or captured by an attacker. We further assume

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

that no nodes are equipped with tamper-resistant hardware due to cost constraints and hence once a node is captured, all the stored sensitive data and cryptographic information will be known to the attacker. We assume that in any case, the base station (BS) will not be compromised by an attacker.

II. THE PROPOSED BIOMETRIC BASED USER AUTHENTICATION SCHEME

In this section, we discuss four phases of our scheme. We use the biometric template pattern matching in our project to perform the user's biometric verification. In our scheme, we store the user's biometric template pattern in the specific system. When the user inputs his/her biometric template in that specific system, it will be matched against the template stored in the system. So, if there is a match, then the user will pass his/her biometric authentication and the user will be considered as a legitimate user. In our project, we make use of the MD-5 hash algorithm as secure one-way function h(·) and DES algorithm for symmetric key encryption and decryption. The message digest (128-bits) of MD-5 algorithm can be used as the key for encryption/decryption in DES algorithm. Fig 1 represents system architecture of the proposed system.

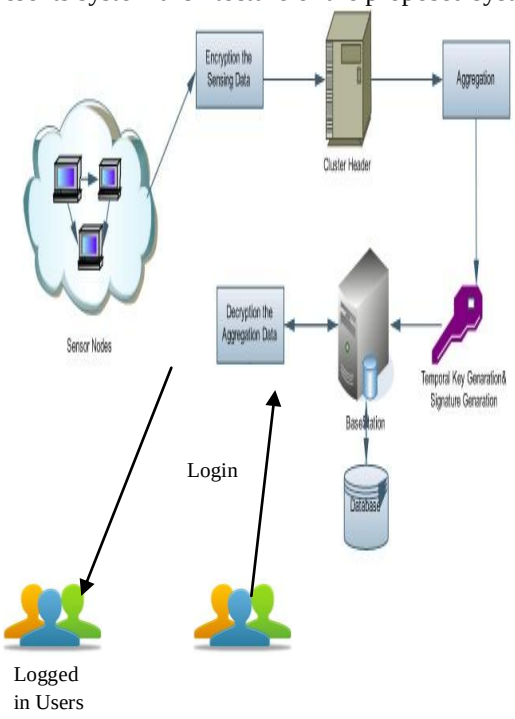

Fig 1: Architecture Diagram

Table I Notations used in proposed system

Symbol	Description
U_i	User
ID_i	Identity of user U_i
PW_i	Password of the user
	U_i
B_i	Biometric of the user U_i
H()	Secure one way hashing
BS	Base Station
S	Secret information maintained by BS only
A||B	Data A Concatenated with Data B
A xor B	XOR operation between A and B
$E_k(M)$	Symmetric encryption of message M under key K
$D_k(M)$	Symmetric encryption of message M under key K
M_{ksj}	Master key of sensor Sj shared with BS
M_{kghi}	Master key of group head shared with BS
RN_x	Random nonce generated by node X

a. PRE_DEPLOYMENT PHASE

We consider a heterogeneous wireless sensor network consisting of two types of sensors: a small number of powerful High-end sensors (H-sensors) and a large number of resource- constrained Low-end sensors (L-sensors). We assume that the target field is two dimensional and partitioned into a number l of equal sized disjoint groups (clusters). Each group G_i will consist of a group head GH_i (here it is an H-sensor node) and an equal number n_i of L-sensor nodes. The group head will be deployed around the centre of the group and L-sensors are deployed randomly in that group. Before deployment of nodes in the network, the base station (BS) does the following steps.

Step 1: The BS assigns a unique identifier ID_{Sj} to each sensor node S_j in each group G_i of the network and a unique identifier ID_{GHi} to each group head GH_i in the network.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

Step 2: The BS then generates randomly a unique master key MK_{Sj} for each S_j in each G_i. Note that the master key is only shared with base station. The BS also generates randomly a unique master key MK_{GHi} for each GH_i. Thus, the nodes are loaded with their assigned identifiers and the master keys before their deployment in the target field.

b. REGISTRAION PHASE

Before accessing data from a particular sensor node in the sensor network, the user U_i needs to register with the BS of the network. This phase consists of the following steps.

Step 1. At first, the user U_i inputs his/her personal biometrics (for example, finger print), B_i, on a specific device and offers his/her password PWi and the identity ID_i of the user to the BS in a secure manner

Step 2. After receiving the password, biometrics and the identity of the user U_i, the BS performs the following: the biometric features of the user's biometrics B_i are transformed using a one-way function $F(\cdot)$ and let $f_i = F(B_i)$, computes $e_i = h(PW_i||f_i)$, and $r_i = h(ID_i||PW_i||f_i)$ XOR $h(ID_i||$ x). Note that the secret information x is only known to the BS.

Step 3. The BS then randomly selects m sensor nodes, say, S_1, S_2, . . . , S_m from different groups and computes its authentication path needed for calculating the root value of that particular node as (ID_i,path) pair.

Step 4. Finally, the BS store the following parameters: (i) ID_i, (ii) r_i, (iii) f_i, (iv) e_i, (v) $h(\cdot)$ and (vi) m ID and path combinations {Path, IDS_j), j = 1, 2, . . .,m}.

c. LOGIN PHASE

In this phase, if the user U_i wants to access data from the WSN, the user U_i needs to perform the following steps.

Step 1. U_i provides his/her personal biometrics, B_i on the specific device.

Step 2. The system verifies the user's biometric template with the biometric templates stored in the database. If the biometric verification does not pass, the user authentication procedure terminates immediately. On the other hand, if the verification holds, the user U_i inputs his/her password PWi and identity ID_i.

Step 3. Next it verifies the identity ID_i and password PW_i of the user with the stored ones on it as follows. It computes $e'_i = h(PW_i||f_i)$ and if $e'_i = e_i$, then the user U_i does not pass the password verification and the user authentication process is terminated. Otherwise, if $e'_i = e_i$, then Step 4 is executed.

Step 4. User U_i generates a random nonce RNU_i and then computes M1 = $h(ID_i||PW_i||f_i)$ XOR RNU_i and M2 = $h(r_i||RNU_i)$, where $f_i = F(B_i)$ is already stored in database.

Step 5. The User selects a sensor node, S_j from its memory from which the user U_i wants to access the real-time data from the sensor network and then produces a cipher text message M3 where, M3 = $Eh(MK_{Sj}||ID_{Sj}||ID_i||S)(M1,M2,RNU_i)$ using the hashed master key $h(MK_{Sj}||ID_{Sj}||ID_i||S)$ of the selected node S_j stored in its memory. Finally, the user U_i sends the message<ID_i, ID_{Sj}, M3> to the BS, via a public channel.

d. AUTHENTICATION PHASE

After receiving the login request message (ID_i, T_i, C_i) from the user U_i, the base station BS performs the following steps in order to authenticate the user U_i.

Step 1. The BS first computes the hashed master key $K_b=h(D_i||T_i)$, of the sensor node S_j received it the message for the user U_i. The BS then decrypts C_i to retrieve $ID_i||RNU_i$ ||<path-1>||root using the computed key. After that the BS will be storing the ID_i and RNU_i for future purposes. These values will be used to prevent ht replay attack. And using the authentication path given it will calculate the root value of the node and also it generates a random number RN_{bs}

Step 2: Using the secret key shared between the base station and the sensor node the base station will encrypt the following information. $M=E_{mk}(RNU_i||RN_{bs}||root)$ and will send (ID_i, ID_s, M)

Step 3: Once this message is received the sensor node will decrypt the message using the master key known only to the sensor node and BS and compare the received root value and the original root value is same or not. And also it stores the value RN_{bs} for preventing the replay attack in the future.

Step4: Once the user is authenticated the sensor node will generate a session key so that the future communication can be done securely and session key $SKui,s=h(ID_i||ID_{sj}||RNU_i||root)$ and sends back the acknowledgement (ID_i, ID_{sj}, $E_{sk}(RNU_i)$).

Step5: When the user receives the acknowledgement the user also will be calculating the session key and decrypts the message and checks whether the random nonce send by the user and received is same or not. If it is same the connection is established and the future communication will be done.

III. SECURTY ANALYSIS OF OUR SCHEME

a. REPLAY ATTACK

Suppose an attacker intercepts a valid login request message (ID_i,T_i,C_i) n the login phase and tries to login to the BS by replaying the same message (ID_i,T_i,C'_i)= (ID_i,T_i,C_i). After receiving such a login request message, the BS computes the symmetric key by hashing its ID and the secret value x known only to the BS. After decrypting the message C_i the BS will check for the random number RN_U

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

in the message However, there will be a match between RN'_{U_i} with RNU_i stored in the BS's database corresponding to the user U_i. The message (ID_i,T_i,C'_i) will be treated as a replay message and the BS will simply discard that message. As the BS keeps track of uniqueness of the random nonce corresponding to each user, our scheme prevents the replay attacks through random nonce.

b. IMPERSONATION ATTACK

On intercepting a valid login request message (ID_i,T_i,C'_i) in the login phase, the attacker will have C_i but, in order to login further to the BS, the attacker needs to re compute C_i with a new random nonce. Otherwise, the message will be detected as a replay one. Now, in order to re compute M3, the attacker must have a idea about the symmetric key used for encryption which is $H(ID_i \| X)$. As the hash function is irreversible and the value of 'X' is only known to the BS, that possibility can be avoided. So, the attacker cannot login to the BS after intercepting a valid login message. Our scheme then resists against impersonation attack.

c. STOLEN VERIFIER ATTACK

In this scheme as the password and the biometric values are not stored in any place. Only during the registration phase the user provides his credentials and after that the base station deletes the values from its memory. And as it is assumed that BS is trustworthy and is unable to compromise this scheme withstand the impersonation attack.

d. GUEST ATTACK

Retrieving password or any other valid information is considered infeasible as the whole data send is encrypted using the proper key. Until and unless the attacker gets any idea about the 'x' which is known to only the BS, the chance of the attacker to make a correct guess is very less. As DES is strong against the guessing attacks the same strength will be available for our protocol also.

e. PASSWORD CHANGE ATTACK

For any attacker it is difficult to derive or change the password because the attacker has to pass the biometric verification. However, the attacker is unable to pass the biometric verification due to the properties of the biometrics, because there will be a mis-match between the attacker's biometric template and the biometric template stored in the system of the original user. Further, in our scheme for changing the password the attacker has to pass the old password verification. For a success in this attack the attacker has to guess the old password before updating the new password chosen by him/her. Hence, our scheme prevents against password change attack.

f. PARALLEL SESSION ATTACK

The BS stores only the value of the latest random nonce in its memory. So as the attacker doesn't have the idea about the key and the he will never be able to alter the message send to the BS and unless and until it happens the chance of parallel session attack doesn't exist.

g. MASQUERADE ATTACK

Easily prevented as the attacker won't be able to decrypt the message Ci and as a result he won't be able to send any valid message to the BS.

IV. RESILIENCE AGAINST NODE CAPTURE ATTACK

In the WSN the sensor nodes can be easily captured and the secret value stored in the sensor nodes can be easily retrieved as the sensor nodes are not made of tamper resistant material. But in our scheme we are sharing a secret master key MK with each sensor nodes and it is assigned by the BS during the post deployment phase itself. And all the communication between the BS and the sensor nodes will be completely encrypted with this master key. So even if the attacker is able to capture the sensor node he won't be able to intercept the messages send to other sensor nodes as those messages will be encrypted using different key.

V. CONCLUSION

In this paper, an efficient Biometric-based User Authentication Mechanism (BUAM) for Heterogeneous Wireless Sensor Networks (HWSN) has been implemented. BUAM have some good properties such as without synchronized clocks and mutual authentication using random nonce. Our scheme also provides non-repudiation because of the characteristics of personal biometrics. We have shown that our proposed scheme is efficient in term of efficiency compared with other related scheme.

VI. ACKNOWLEDGMENT

The author would like to thank, Mrs. Sreedevi N, Head of the Department of Computer Science & Engineering, MVJ College of Engineering, Bangalore, for her immense support over preparing this paper.

REFERENCES

[1] Ashok Kumar Das and Bezawada Bruhadeshwar. A Biometric-Based User Authentication Scheme for Heterogeneous Wireless Sensor Networks.

[2] M. L. Das. Two-Factor User Authentication in Wireless Sensor Networks. IEEE Transactions on Wireless Communications, 8(3):1086–1090, 2009.

[3] T.-H. Chen and W.-K. Shih. A Robust Mutual Authentication Protocol for Wireless Sensor Networks. ETRI Journal, 32(5):704–712, Oct. 2010.

AUTHOR BIOGRAPHY

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

Srikanth S P is a Computer Science Engineer, presently working as an Assistant Professor in the department of Computer Science & Engineering of MVJ College of Engineering, Bangalore. He completed M.Tech from VTU Belgaum University (2004) in IT, and B.E. from Mysore University (1997) in IT.

Deepika S Haliyal completed B.E in computer Science from B.V Bhoomaraddi College of Engineering Hubli, Karnataka, India in 2011 and pursuing M.Tech (CSE) in MVJ College of Engineering Bangalore, Karnataka. Her research interests include information security, Data Mining.