ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Approach for Authentication Technique in Wireless Sensor Networks

D. Prasad
Research Scholar,
Annamalai University, Chidambaram,
Associate Professor,
Ramanandatirtha Engineering College, Nalgonda.

E. Satheesh Kumar
Associate Professor,
Ramanandatirtha Engineering College,
Nalgonda.

Abstract: ***Authentication of user in Wireless Sensor Network (WSN) needs research and investigation due to all the characteristics of these networks, such as limitations of power, computation capability and storage resources with the increasing security threats and attacks. All of the popular User Authentication (UA) schemes in WSN are provide only log in time authentication and for checking the authenticity of user no biometric (physical) property of user is applied. In this paper, we enlighten different new approaches that can be effectively used as a UA scheme in WSN.***

In general the authentication technique in 2G mobile communication is solely dependent on checking the authenticity of MS (Mobile Station or Subscriber) by challenge/response mechanism. Here authenticity is one-way for which MSC (Mobile or Main Switching Center) checks the validity of MS. 3G mobile communication works on two different switching techniques. One is circuit switching for voice and low speed data communications. The other one is packet switching mainly for data communication, but can afford voice communication like VoIP (Voice Over Internet Protocol), video telephony, multimedia service etc. Generally high speed data communication is established by packet switching process through PDSN (Packet Data Serving Node) servers. In circuit switching (3G network) authentication is mutual where both MS and MSC or network authenticate each other, but in packet switching only network (servers in PDSN) examines the authenticity of MS. In this paper, we enlighten different new approaches that can be effectively used as an authentication tool in 3G mobile communications.

Keywords: ***Authenticity of Mobile Station or Subscriber, Challenge/Response Mechanism, Circuit Switching, Identifier, Packet Switching, PDSN, Password.***

INTRODUCTION

A WSN is collection of a set of small sensor nodes/devices and one or more base stations which acts as gateways between Internet users and sensor nodes. Base station centralizes the data gathered by sensor nodes. Sensor nodes are scattered in cluster based topology and have limited communication capabilities with short coverage distance. An assorted set of applications for WSN encompassing different fields including agriculture, environment, medicine, military, motion tracking, machine malfunction, toys, forestry, vehicles and many others.

The influence of the Internet and IP technology has extended to enlighten the cellular area in high speed data transmission [1]–[5]. Data rates reach upto 2 Mbps or more for 3-G mobile communications, opening opportunities forextensive wireless multimedia services. Enabling packet data services off the RAN (Radio Access Network) in UMTS (Universal Mobile Telecommunication System in USA) and by passing the MSC is the beginning step for separating the circuit based world of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the PSTN and the packet based world of PDNs (Public Data Networks) and the Internet [6]-[9]. The European counterpart of UMTS is WCDMA (Wideband Code Division Multiple Access), generally marketed as 3GSM. The WCDMA scheme has been developed as a joint effort between ETSI and ARIB (Japanese) during the second half of 1997, whereas, in March 1998, the TIA (Telecommunications Industry Association) TR45.5 committee, adopted an innovation for wideband CDMA, compatible with IS -95, which is called CDMA-2000. This 3-G network can provide circuit switched voice service, circuit switched data service like 2-G (CDMA One or GSM), in addition to this, packet switched data service [1]. The packet switched can be enhanced in different speeds such as 38.4 kbps, 76.8 kbps, 153.6 kbps, 307.2 kbps, 614.4 kbps, 921.6 kbps, 1228.8 kbps, 1843.2 kbps, 2457.6 kbps etc. There are different control channels e.g. MAC channel, Reverse Traffic Channel, Access Channel etc which are associated to and fro MS to MSC or PDSN to set up the communication path implemented by proper authentication scheme.

Existing System:

The basic user authentication scheme in WSNs was based on public key cryptography where user can authenticate with any subset of sensors out of a set of sensors and it was firstly designed by Benenson et al. in 2004 However, Benenson et al.'s scheme requires that each pair of nodes share a secret key which leads to high storage space and suffers from the problem of scalability. In addition, the scheme is defenseless to capture attacks and it doesn't attend to the case where the node responsible of processing the query is compromised and thus can send error information Banerjee et al. proposed a symmetric key based authentication scheme (converse to Benenson et al.'s scheme) that eliminates the problem of all nodes reply to the user's query. This scheme is sharing pair-wise key, based on Blundo et al.'s techniques but can't be able to determine sensor, involved in the user's query. Moreover, the scheme is vulnerable to node compromise and it doesn't afford mutual authentication (user and network can authenticate each other).

Krik H.M. Wong et al. designed a dynamic user authentication protocol in 2006. They also showed that their protocol can protect login message replay attacks and insider attacks. But the protocol is vulnerable to many logged in users with the same login identity and suffers from stolen verifier attack.

A distributed user authentication scheme based on the Self-Certified Keys cryptosystem (SCK) was developed by Jiang et al. in 2007.

Disadvantages:

• Their scheme allows local nodes act collaboratively to verify whether a user has the authorization to access the sensor network or not. Here, each node receiving this access request from a user, must compute a pair wise key, shared with this user and an encrypted nonce. This is very expensive operation for a small local node in WSN and its decreases the suitability for practical use.

• After that, there is history of advancement of user authentication technology in WSN. Several new user authentication schemes have been pointed.

Proposed System:

The entire packet switched mobile network authentication and improvements provide only one-way authentication i.e. only Servers in PDSN can check the authenticity of a user. The user can not check whether he is communicating with a correct server in PDSN or not. It is a vital gap where a potential adversary can spoof the servers in PDSN and get valuable user information. This motivates to construct an authentication scheme for packet switched mobile network that provides user and server authentication and the user gets access to the network resource only if <user,server>'s authenticity is passed correctly.

Advantages:

The authenticity of user can be checked by different entities as in following procedures:

(i) Using log identifier with password for authentication of mobile subscriber.

(ii) Certified authority server checks the authenticity of subscriber (MS).

(iii) Different biometric authentication is a technique to check a valid user by user physical characteristic. Human physical characteristics are called Biometric property such as Fingerprint, Voiceprint, Retinal scan and Face recognition etc.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Out of these biometric characteristics, we emphasis on following areas:

(A) Acoustic Recognition: In this process, sound detecting from ear of the mobile subscriber (MS) is done by biometric authentication method. Ear not only senses sound but also makes signals of its own called OAEs (Otoacoustic Emission). These OAEs are produced by the motion of hair cells within the outer part of the spiral shaped cochlea lying in the inner ear. Hearing is an active process where the ear actually puts energy into the incoming sound waves to replace energy lost as sound which is absorbed by the ear's function. Due to this process some of the energy added by the hair cells escape as OAEs. These OAE signals are detectable by supersensitive (ultra low noise) microphone. These signals prove unique to each individual including male, female etc. Thus this can be used as an authenticity marker for a caller or set of callers using MS to the network either in circuit or packet switching cases. Hence the use of stolen mobile can be automatically disabled in case of the users are not legitimate owner by simply matching the stored specimen of OAEs.

(B) Face recognition: Face images of the mobile equipment (MS) users are stored either in AUC or PDSN server. The MS (mobile caller) is authenticated by matching the face image of actual user with that of the notified users in MSC or PDSN database. If these two images are completely matched, the call will be progressed, otherwise not. Authenticity of the network or server (MSC or PDSN) is identified by MS through the following procedure:

(i) Response and throughput time of the server.
(ii) Shared secret key pairs between the user and the server.
(iii) Received power level from the server.

Authentication In Mobile:

GSM (2-G) networks utilize authentication for verifying authenticity of subscriber [3]-[5]. Each subscriber is identified with a unique IMSI (International Mobile Subscriber Identity) number. He has a unique subscriber authentication key (Ki).The authentication algorithm used in the GSM system in 2-G is known as the A3 algorithm. The SIM (Subscribe Identity Module) contains the IMSI, Ki and A3 algorithm. The AUC (Authentication Center) contains the A3 algorithm as well as a database of authentication information about the subscriber. A3 actually generates 128 bits of output. The first 32 bits of those 128 bits form the Signed Response. The A3 algorithm is implemented in the SIM (Subscriber Identity Module).

Authentication in the GSM network utilizes following Challenge/Response mechanism,

1. The HLR (Home Location Register) generates a 128-bit RAND (Random Challenge).

2. The HLR sends RAND to the MSC (Mobile Switching Center).

3. The MSC sends it to the BTS (Base Transceiver Station).

4. The BTS sends it to the MS (Mobile Station).

5. The MS receives it and generates 32-bit SRES* (Signed Response) utilizing RAND and the 128-bit Ki from the SIM (Mobile Station's Subscriber Identity Module) utilizing the A3 algorithm.

6. The MS sends the SRES* to the BTS.

7. The BTS sends the SRES* to the MSC.

8. The MSC checks whether SRES = SRES* or not. If they are same, MS is authentic. This process authenticates the MS (Mobile Station) to the GSM or CDMA-One network. One known security limitation of 2-G networks is that the network is never authenticated by the MS (Mobile Station). This one-way authentication makes it possible for an attacker to pretend to be a network provider. As 2-G mobile authentication mechanism is only one way, therefore the user is not given the assurance that they have established a connection with an authentic serving network.

B. Authentication for Packet Switching in 3G network:

Authentication for packet switching is done by AAA (Authentication, Authorization and Accounting) server Authentication requires the user to provide an account number or identifier and password i.e. exchange of logical keys or certificates between the client (MS) and the server in PDSN. If this authentication is correct, then MS is permitted for

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

packet data service by Authorization. An AAA server is a server program that handles user requests for access to network resources. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

Conclusion:

3-G mobile network is completely described above with the present authentication scheme. It is seen that wireless communication is enhanced in packet switching technology, as a result high speed secured data as well as voice transmission-reception is possible. Our future work is to invent new efficient mutual authentication technique using entities like Password, Identifier, Certified Authority, Biometric Property etc. of the subscriber in both circuit switching and packet switching mobile communications.

References:

[1] C. T. Bhunia, Information Technology Network and Internet, New Age International Publishers, India, 5th Edition (Reprint), 2006.

[2] William C. Y. Lee, Wireless and Cellular Communications, 3rd Edition McGraw Hill Publishers 2008.

[3] P. K. Bhattacharjee, "A New Era in Mobile Communications- GSM and CDMA" in National Conference on Wireless and Optical Communications (WOC-07) at Punjab Engg College (D.U), pp 118- 126, on 13th- 14th Dec, 2007.

[4] T. S. Rappaport, Wireless Communication: Principles and Practice, Prentice Hall Pub Ltd, 2nd Ed, 2006.

[5] P. K. Bhattacharjee, "Hybrid GSM And CDMA Mobile Communication Systems Enhancing Channel Capacity" National Conference on Wireless and Optical Communications (WOC-08), Punjab Engineering College (Deemed University), Chandigarh with IEEE, pp 1-8, from 18-19th Dec, 2008.

[6] D. Goodman, "Cellular Packet Communication", IEEETransactions on Communications, vol. 38, no. 8, pp. 1272-1280, August1990.

[7] S. N. Diggavi, N. Al-Dhahir, A. Stamoulis, R. Calderbank, "Great Expectations: The Value of Spatial Diversity in Wireless Networks, " Proceedings of the IEEE, Volume 92, Issue 2, pp. 219–270, Feb 2004.

[8] P. Ramjee, O. Tero, "An Overview of CDMA Evolution towards Wideband CDMA", IEEE Communications Survey, 1998.

[9] F. Adachi, M. Sawahashi, H. Suda, "Wideband DS-CDMA for Next Generation Mobile Communications System", IEEE Communication Magazine, pp 56-69, Sept, 1998.