A Noval Approach for substantiation Protocol with Time Scheduling


K.Vinoth, Assistant Professor, PRIST UNIVERSITY, Thanjavur

ABSTRACT

Security in Personal Area Networks (PAN) is even more challenging. Increasingly, companies and individuals are using wireless technology for important communications they want to keep secure data transmissions. We propose a method that allows Service provider (server) to send a One Time Password (OTP) for the secure communication so the data transmission can be accessed by primary users more authenticated. In the existing method, a malicious secondary user (hacker) who wants to gain an unfair use of a data in the network can emulate the primary user, and can thus trick the other secondary users into believing that the primary user. For that the real time experiment, we demonstrate using ZIGBEE network and GSM Module, it having one server, one access location that refers the node, when the user enter to this network, first of all request send to the access location then that node intimate to server will check whether that node is the authorized person or not. If the node is authorized then the OTP password send to that person and after comparing the password the data transmission and data connection will be establish. It is possible to apply similar security concept for a military, Industrial, E-Commerce, Medical and Scientific applications.

KEYWORDS: OTP (One Time Password), User Node, Service Provider, Zigbee, GSM (Global System for Mobile Communication), Security in personal area network (SPAN).

I. INTRODUCTION

The project aims to establish secure wireless communication between service provider and users. The issue of security of the communication is addressed by ZIGBEE technology and GSM module. The secure OTP is transmitted over the wireless using GSM module. If the user is authorized, then the network will be enable for initiate the data transmission. The network security is becoming more important as the amount of data being exchanged on the Internet is increasing. Security requirements are necessary both at the final user level and at the enterprise level, especially since the massive utilization of personal computers, networks, and the Internet with its global availability. Throughout time, computational security needs have been focused on different features secrecy or confidentiality, identification, verification, non repudiation, integrity control and availability. This has resulted in an explosive growth of the field of secure personal area network. ZIGBEE is flexible in performance and is battery operated ZIGBEE protocols are anticipated for embedded applications that require low power and low cost. GSM is a cellular network, which means that mobile phones connect to it by searching for
cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average roof top level.

II. RELATED WORKS
In this existing project, we present a robust one-time authentication protocol, based on two cryptographically strong building blocks, namely, the Authenticated Key Exchange key exchange and the keyed Hash Message Authentication Code (HMAC), that provides several advantages with respect to most of the available solutions at the state of the art. Authentication techniques based on OTP are typically implemented by means of four phases, each implemented by an appropriate algorithm. In particular, the Key Setup deals with the generation of session keys, the Key Scheduling takes care of selecting the session key to use for authentication, whereas the Key Update is responsible for updating the set of session keys to be used and finally, the Authentication implements the whole protocol logic.

End-to-End low complexity OTP-based authentication protocol, which provides non-interactive Key Scheduling and Key Update, is transparent to the user, and results to be cryptographically strong against state-of-the-art known attacks. Such protocol is composed by four algorithms, respectively denoted by Key Setup, Key Schedule, Key Update and Authenticate which have to be implemented by both the involved endpoints. Simply stated, the proposed protocol operates as follows. After agreeing on a common Master Key by using an Authenticated Key Exchange (AKE) scheme. Both the involved endpoints, starting from such key, independently generate a set of session keys, having the same size of the Master Key. Emphasize the fact that the use of AKE instead of the basic one (such as Diffie-Hellman) is due to the well-known vulnerability of the latter one against the Man-in-the-Middle attacks. Then, the endpoint which wants to access a specific resource, selects a session key from such set (Key Scheduling). It is important to emphasize that such key will be scheduled independently but in an identical manner by both the endpoints through the use of the previously agreed Master Key. When the right session key has been selected, the Authentication may proceed and the authenticating endpoint sends to the other party, into an authentication request message, the currently selected session key. The endpoint which holds the resource verifies if the received session key is correct, i.e., whether it is valid and it has been scheduled at the appropriate time. If both the conditions hold, then the authenticating endpoint is allowed to access the requested resource.

Advantage
- Relative simple and limited overhead, it is able to operate indistinctly in a wide range of
scenarios, without requiring particular changes

- Low complexity is mainly due to two main factors, the former related to the efficiency of involved cryptographic primitives, while the latter concerning the small number of messages exchanged, in order to carry out Key Setup, Key Schedule, Authentication and Key Update phases.

**Drawbacks**

- The protocol is particularly suited for capacity-constrained mobile devices in application not applicable to network.
- Existing algorithm do not works effectively against the attacks of the nodes in the network.
- It cannot be implemented in the hardware implementation. It does not include any hardware modules.
- Unauthenticated person easily access the data and disables the network, because it operates in program level.
- Slow down network performance via bringing the network down for long time.

## III. ANTICIPATED SYSTEM

The proposed method does not allow the attacker to discover the network path. In the proposed system allows the service provider to send the OTP to the relevant user, who wants to get the data from the server. So the authenticated users only access the data from the network. This OTP can be generated in the random manner and varied based on the reputation access. Authentication can be done in various levels including wireless access point using the ZIGBEE protocol and transmission of password can be achieved through the GSM module.

The main concern for this project is the cost induced on the users hardware setup. We uses two technology ZIGBEE and GSM for demonstrate the effectiveness of our project. ZIGBEE is a wireless technology designed to address the unique needs such as affordability and power conservation. It is easy to implement and needs little power to operate. ZIGBEE operates at the radio frequency of 2.4 GHz, which is used to deliver a reliable data and easy to use standards in the entire world. GSM technology defines circuit switched system and divides each 200 KHz signal into 825 KHz time slots and operates in 900 MHz, 800 MHz and 1.8GHz bands, respectively. It uses a narrow band transmission technique – basically Time Division Access Multiplexing.

## IV. BACKGROUND DESCRIPTION

### SERVICE PROVIDER

Server section which enables OTP & allow authorized user for data transmission. Servers send the OTP to the requesting User who wants to enable the data transmission. It includes GSM module, PIC controller, ZIGBEE and power supply. Access node is nothing but the Service provider to initiate the data transmission to the User. It also shows the Users name in the LCD display.
One time Password generation is based on the clock signal generated in the oscillator. Crystal oscillator is used for generating otp, since there is low modulation in the frequency. The main function of the oscillator is to generate a 1/32 Hz clock signal which is used to increment a 24 bit binary counter. The counter can be read over the serial interface and can also be set to any desired value. Control over the divider chain also allows for accurate starting of the counter. Incrementing of the counter value during read is prevented by freezing of the counter during access. An interrupt signal is also available and is triggered coincident with the counter updating. This signal can be used as a wake-up for a microcontroller.

Generated password is send to the user node by zigbee transmitter, Authorized user details is stored in the module. After verification of the password from the user node, data transmission is enabled.

**USER NODE**

User node send data transmission request through keypad, by sending the authorized user details such as user name & password, details is transmitted through zigbee, after verification of user details in server section one time password is transmitted to mobile device through GSM. otp is transmitted to the server section, it the Otp is valid data transmission is enabled otherwise not.

V. RESULT AND CONCLUSION

- The performance will be effective based on the ZIGBEE protocol and gets OTP at the required time through GSM module.
- Unauthorised person cannot access the data from the network and also guess the password is difficult because it’s varies with time.
- The network performance and data transmission level will be good because this can be handled by single user.
- It cannot depend any algorithm and application level. So it can be easily execute in the real time process.

Anovel OTP-based authentication that overcomes several problems affecting many of the existing solutions. First of all, this protocol results to be efficient, both in terms of involved operations and number of messages that is transmitted in the network is unique &
unpredictable. It is highly secured Data transmission in the network since one time password changes with time and it is unpredictable by third party. Unauthorized person cannot acess the network with out authentication from server. OTP are widely used as a log-on authentication methodology in a variety of Internet services.

The time synchronization format that automatically generates passwords over fixed time intervals, and the challenge and response format, where a response is generated as a result of computations by a predetermined set of random digits - the challenge - from by the administrator. Real time execution is possible and suited for mobile & Network access. It provide high secured data transmission in the network.

VI. FUTURE ENHANCEMENT

OTP automatically generates passwords over fixed time intervals, and is used in various internet log-on authentication scenes, such as internet banking transactions. In addition to such domestic markets as the financial sector, including banks, insurance companies and internet-based securities brokers, and the on-line game sector,

It will also actively expand event-driven format and time synchronization format cards for the overseas market. And as smart phones, which continue to see rapid increases in usage, also require security measures on the same level as computers, There is a expansion in the OTP market targeting companies.