ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

Lightweight anonymous authentication protocol for secure wireless sensor network

Ms.S.Thilsath banu M.E., Assistant Professor /ECE

P.S.R.Rengasamy college of Engineering for women

E.Aathi Lakshmi
aathisri96@gmail.com,9488059588,

A.Priyanka
priyaalagar096@gmail.com.98798747412,

S.Gowthami Rajeshwari
gowrikowsi5@gmail.com,8524014907,

P.S.R.Rengasamy college of Engineering for women

Abstract:

Wireless sensor networks (WSNs) are becoming more and more popular in everyday life. These wireless sensor can be quickly and easily deployed in hostile environments, and wireless sensor networks are now widely used in a variety of real-time applications, such as vehicular tracking, habitat monitoring, environment control, military surveillance, healthcare monitoring, wildlife monitoring, and traffic monitoring. We propose a secure mutual authentication scheme a cover-coded pad function to protect the data. It can authenticate to an accessed node and vice versa. It is to ensure that data transmission is not hacked by an unauthorized person. On the other hand, it ensures that data sent to sensor did not originate from a malicious node.

Index Terms: Mutual authentication ,user anonymity,security,WSN.

INTRODUCTION

Wireless sensor network is a kind of autonomous network with sensor nodes. It is concerned with people trying to access remote services that they are not authorized to use. The security of information felt to be valuable to an organisation. To distinguish legitimate users from intruders, authentication techniques are frequently used to verify the identity of the participants in a communication system.

A Wireless sensor network consists of spatially distributed autonomous sensor to co-operatively monitor physical or environmental conditions. In WSN, it offers a limited amount of data reusability as local results from each participating node are passed to the base station. However, WSN are highly vulnerable to the failure of base stations. This is because the WSN itself a transmit messages through the wireless communication media. The attacker can access to make anonymity connections and the message is vulnerable to eavesdropping, interception and tampering. In WSN, the message exchange through wireless access, if the information is not transmitted through the protection process, data messages will easily be stolen or received the fault messages. It is very important to protect the confidentiality of information and privacy for WSN. Therefore, mutual entity authentication plays an important role in securing WSN.

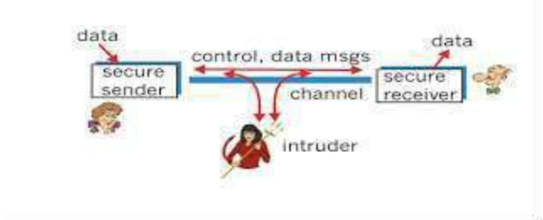


Fig:1 Real time access in WSN

A.Security Requirements:

Secrecy: Only the sender and intended receiver should me able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message be some how encrypted so that an intercepted message cannot be decrypted by an interceptor .

Authentication : Both the sender and receiver to confirm the identity of other party involved in the communication to confirm that the other party is indeed what the client to be.

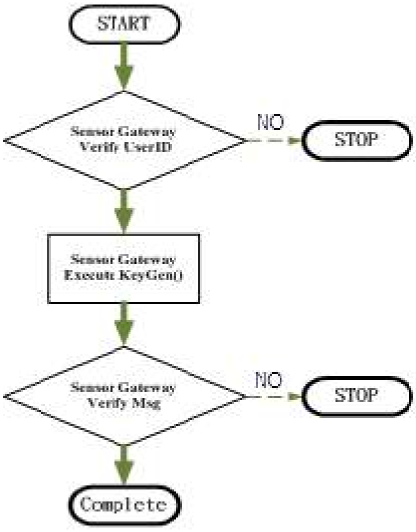

START
Sensor Gateway Verify UserID
NO
STOP
Sensor Gateway Execute KeyGen()
Sensor Gateway Verify Msg
NO
STOP
Complete

Fig:2 Authentication

Message Integrity: Even if the sender and the receiver are able to authenticate each other they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extension to the checksum technique that we encountered in reliable transport and data link protocol.

Non Repudiation: It deals with signatures. The sender wants to send data to the receiver in secure manner. All, or some of this message will typically be encrypted. A passive intruder can listen to and record the control and data messages on the channel. An active intruder can remove messages from the channel and itself add messages into the channel.

Problem statement: Anonymity in sensor networks means preventing a third party from knowing the identity of the two primary parties during communication.. Each node plays a different role in the network. A source node is a sensor close to the event spot and generates messages to the base stations. Normal nodes on route are responsible for message relay. The base station is the controller of the network and carries out many tasks. An important node such as a source node plays a critical role in the network. A smart attackers may first try to identify important nodes and then compromise these nodes, which can cause damage to the network. Node identityand anonymous communication can prevent the above selectively attacks. Anonymity in the context of a sensor network includes sender anonymity, receiver anonymity and unlink ability between the sender and the receiver. With the anonymities, an adversary is not able to determine the sender and receiver's identities by reading a message intercepted from the network forwarded by a compromised sensor node. The adversary cannot determine whether two transmission are relaying the message either. We proposed several effective anonymous schemes that can hide node identity and relay message between sensors and base station. Our anonymous schemes can be used with any existing sensor routing protocols. [7] discussed about a method, End-to-end inference to diagnose and repair the data-forwarding failures, our optimization goal to minimize the faults at minimum expected cost of correcting all faulty nodes that cannot properly deliver data. First checking the nodes that has the least checking cost does not minimize the expected costin fault localization. We construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. We proposes efficient inferring approach to the node to be checked in large-scale networks.

Paper organization: Therefore, the reminder of this article is organized as follows. We present our anonymous user authentication protocol for WSN environment. The abbreviations and cryptographic functions used in this article
are defined in the TABLE I.

TABLE I
NOTATIONS AND CRYPTOGRAPHIC FUNCTIONS

Symbol	**Definition**
U	User
GW	Gateway
Sn	Sensor
IDU	Identity of the user
AIDU	One-time-alias identity of the user
SID	Shadow identity of user
IDG	Secrect Identity of the gateway
□	Secret key of the gateway
Snid	Identity of the sensor node
PSWU	Password of the user
Nu	Random number generated by the user
SK	Session key between Sn and U
Kug	Shared key between U and GW
Kem	Shared emergency key between U and GW
Kgs	Secret Key shared between the GW and Sn
Tsug	Transaction sequence number

(maintain both U and GW)

h(.)	One-way hash function
□	Exclusive-OR operation
||	Concatenation operation

PROPOSED SCHEME:

We will describe our proposed realistic anonymous authentication scheme in detail. Our proposed scheme consists of four phases .In phase I a gateway issues a smart card to an intended user through secure channel, this phase is called Initialization phase. The next phase of our proposed scheme is the neighbour node calculation it is used to find the nearest neighbour to find the data. In phase III is file transmission in dynamic in this phase data transmission can be done. In phase IV it is used to eliminate attackers, unauthorized person can be hacked in this phase. The objectives of our proposed scheme are as follows:

To achieve mutual authentication by preserving the feature of user anonymity :

To achieve untraceability;

To achieve perfect forward secrecy(PFS);

To defeat forgery attack, known session key attack long with the forward/backward secrecy support;

To reduce computation and communication cost;

To offer a realistic and expeditious solutions;

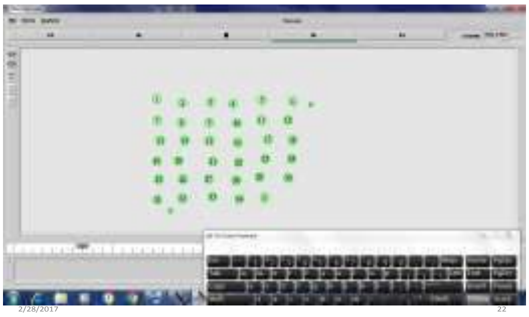
Phase I: Initialization phase

In this phase, a user submits his/her IDU and a hash of his/her password to GW via a secure channel. Then, GW issues a license to U. The steps are described as follows:

Step 1 : User enters an identity, selects a random number and a password. Then users send message via secured channel

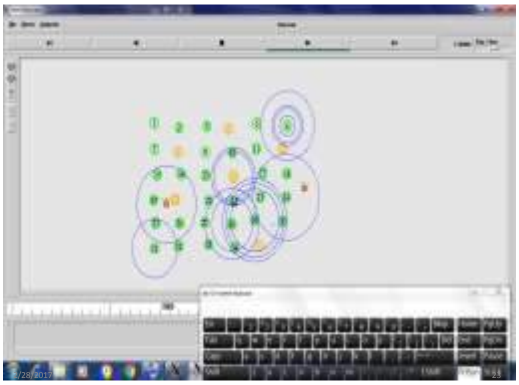
Step 2: After receiving the request the gateway (GW) generates the transaction sequence number. This sequence number is computed based on the number of request handled by the GW, including the present request of current user. The concept of sequence number is mainly used speedup the authentication process as well us to prevent any replay attempt from any adversary.

Registration phase



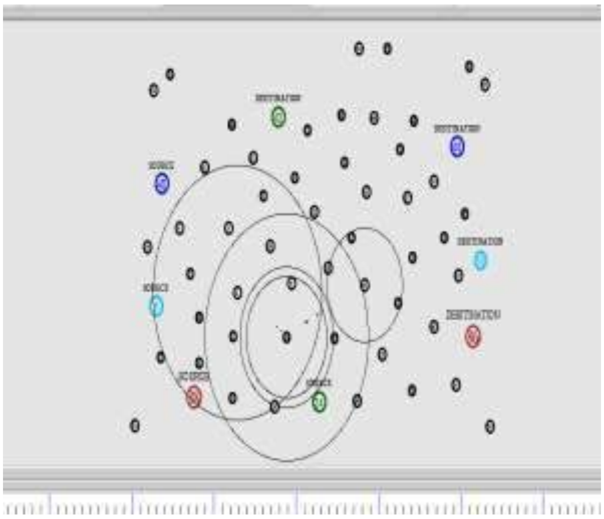
Neighbour node calculation:

We present a novel an effective method to calculate nearest neighbour node in WSN, which enable each node to find the kth nearest neighbour node and adjust transmitting range according to local requirement.



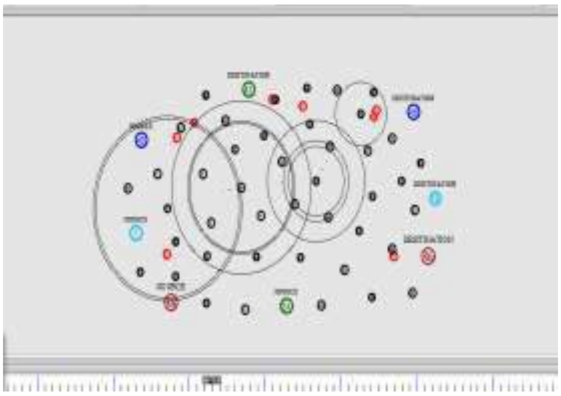
File transmission in dynamic:

A Wireless communication device dynamically determines the number of wireless network parameter prior to data transfer to increase network efficiency and decrease delays during the transmission of a multimedia messaging service message.



Eliminate attackers:

In the existing phase, there is possibility for loss of data or packet. Because, there is a possibility to hack the data by the intruder . But in our, proposed scheme, there is no possibility to hack the data. By identifying the intruder and eliminating them we can send data ina secure manner.



Security analysis:

Mutual Authentication:

Our scheme provides mutual authentication, where all entities are mutually authenticating each other. More specifically, when the GW node receives the message it can make sure that the user message is included in the sensor node message. When the sensor node receives message, it ensures that this message is generated by the GW node. Furthermore, when the user receives message he can also confirm that this message is generated by the sensor node. Hence, mutual authentication is achieved.

Replay Attacks:

Our scheme is resistant to replay attacks, because the authenticity of messages is validated by checking the freshness of four time stamps. Let us assume an intruder intercepts a login request message and attempts to access the sensor node by replaying the same message . The verification of this login attempt fails since the time difference expires. Similarly, if an intruder intercepts a valid message and attempts to replay it to the GW node, the verification request will fail at the GW node because the time difference expires again Thus, our protocol is secure against replaying of messages.

Stolen-Verifier Attacks:

An attacker who steals the password verifier from the gateway can use the stolen verifier to impersonate a legal user to login to the system. The proposed scheme is free from the stolen verifier attack. There is such information stored at the server, by which an adversary can make a fabricated login request to impersonate a legal user to login the server or can impersonate the gateway to cheat the legal user and the sensor node.

Password attack:

In this attack an adversary tries to login with guesses password. Two popular methods for this attack are dictionary attack and brute force attack. In brute force method, an adversary tries with all possible combinations. In dictionary method, an adversary tries with a word list of potential passwords.

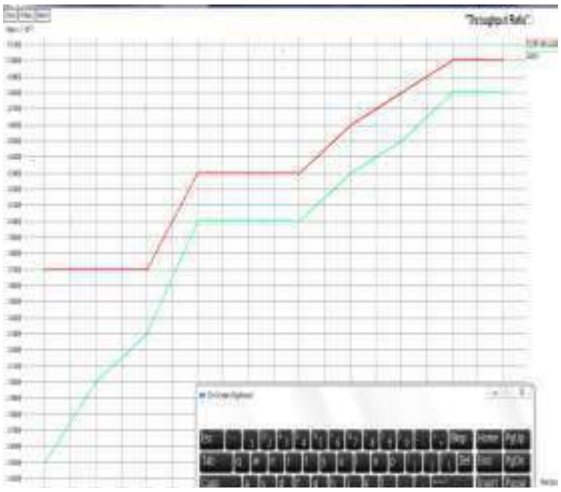
PERFORMANCE ANALYSIS AND COMPARISONS:

The proposed scheme is to resolve several security issues existing in the authentication environment of the wireless sensor network and simultaneously to offer a solution. In this section, we compare our proposed scheme with recently proposed scheme with user anonymity manifest the advantages of our propose scheme. In our proposal scheme and the protocols presented and a sensor node needs to perform hash operations. For the security of these protocol we consider that the hash function used in proposed scheme. It requires only hash operations. It can be easily stated that, the computational overhead of the proposed scheme is significantly less. The length of the identify of the sensor node is 128-bit, the length of the each hash value is also 128-bit, and the length of the timestamp value is 24-bit. Which is significantly higher than both the proposed scheme where for average transmission cost for each byte of data in sensor node Conclusively, the proposed scheme in terms of security, computational overhead, and communication overhead is better. It should be noted, in proposed scheme using number a GW each users request from others. Our proposed scheme is more realistic than the other state.

Throughput:

Throughput is the maximum rate of production. When used in the context of communication networks, such as Ethernet or packet ratio, throughput or network throughput is the rate of successful message delivery over a communication channel.

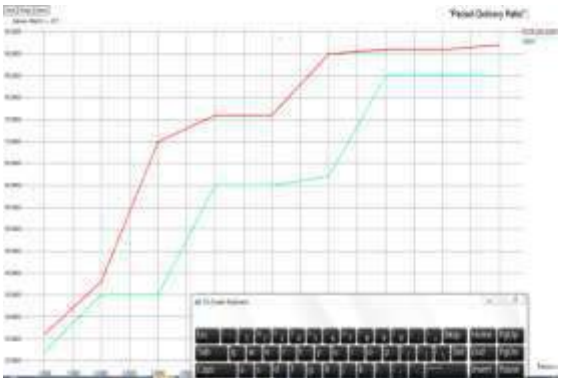
Fig :3 Throughput delay



Packet Delivery Ratio:

Packet delivery ratio is based on the received and generated packets as recorded in the trace file.It is defined as the ratio between the received and generated packets.

Fig:4 Packet delivery ratio



Average end-to-end delay:

Ed-to-end delay or one-way delay(OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from round-trip time(RTT).

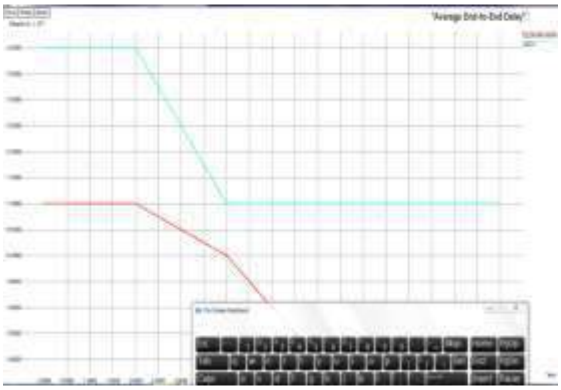


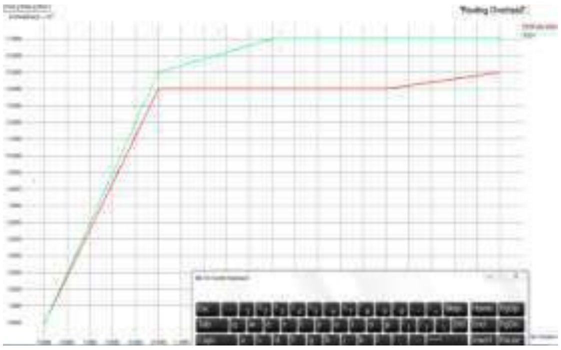
Fig 5: Average end-to-end delay

\

Routing :

Routing is the process of selecting a path for traffic in a network. A router is a networking device that forwards data packets between computer networks. The process of moving a packet of data from source to destination. Routing is usually performed by a dedicated device.

Fig:6 Routing



Conclusion :

In the article, we hav proposed a anonymous user authentication in wireless sensor networks. In comparision with existing schemes, our proposed scheme not only provides more security features and high security level,but at the same time also has low costs of communication and computation. Accordingly, our proposed is suitable for the legitimate user to access sensor data from any sensor node in the environment of constrained wireless sensor network

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. S. Subramaniam, E. Cayirci, "Survey on sensor network," *IEEE Communication Magazine*, vol.40, pp. 112-114, August 2002.

[2] O. Gnawali, K.-Y. Jang, J. Paek, M. Vieira, R. Govindan, B. Greenstein, A. Joki, D. Estrin, E. Kohler, "The tenet architecture for tiered sensor networks," *in: Proc. SenSys* 2006, ACM, pp. 153–166, October 2006.

[3] D. Yang, S. Misra, X. Fang, G. Xue, J. Zhang, "Two-tiered constrained relay node placement in wireless sensor networks: computational complexity and efficient approximations," *IEEE Trans. Mobile Computing*. vol. 11 no. 8 pp. 1399–1411, August 2012.

[4] P. Gope, T. Hwang, "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network," *IEEE Sensors Journal*, Vol. 16 (5), pp. 1368 – 1376, March 2016.

[5] T. Nguyen, A. Al-Saffar, and E-N Huh, "A dynamic ID-based authentication scheme," Proceedings of the Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp. 248-253, August 2010.

[6] P. Gope, T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," *IEEE Sensors Journal*, vol. 15 (9), pp. 5340 – 5348, June 2015.

[7] Christo Ananth, Mary Varsha Peter, Priya.M., Rajalakshmi.R., Muthu Bharathi.R., Pramila.E., "Network Fault Correction in Overlay Network through Optimality", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Volume 2, Issue 8, August 2015, pp: 19-22

[8] M.L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transaction on Wireless Communications*. vol. 8 no. 3, pp. 1086– 1090, March 2009.

[9] D. He, Y. Gao, S. Chan, C. Chen, J. Bu. "An enhanced two-factor user authentication scheme in wireless sensor networks," *AdHoc & Sensor Wireless Networks* vol. 10 no. 4, February 2010.

[10] H. Yeh, T. Chen, P. Liu, T. Kim, H. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors,* vol. 11, no. 5 pp. 4767–4779, May 2011