GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ENHANCED SECURITY PROTOCOL FOR USER AUTHENTICATION IN WIRELESS SENSOR NETWORK

MAHALAKSHMI.G
School of computer science, Engineering & Applications
Bharathidasan University

ABSTRACT

If the data collected within a sensor network is valuable or should be kept be confidential then security measures should protect the access to this data. We focus on user authentication, a central problem when trying to build access control mechanisms for sensor networks.

Keywords: wireless sensor network,user authentication,security.

I. INTRODUCTION

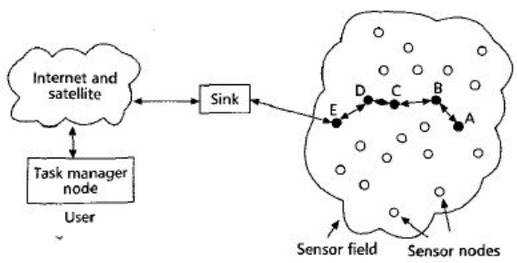
A wireless sensor network (WSN) can cheaply monitor an environment for diverse industries, such as healthcare, military, or home [. A WSN typically consists of several base stations and thousands of sensor nodes, which are resource limited devices with low processing, energy, and storage capabilities. Distributing data through wireless communication is also bandwidth limited. User authentication is a basic and important security mechanism in a WSN.

II. PROBLEM STATEMENT

In general, whenever sensor nodes process a query, they should be able to verify that the query comes from a legitimate user. We call this problem authenticated querying.More formally, a WSN enables authenticated querying if it satisfies the following properties (perhaps, with some large
probability):
_ Safety: If a sensor s processes the query q, then q was
posted by a legitimate user U.
_ Liveness: Any query q posted by a legitimate user U is processed by at least all sensors s 2 Sq, where Sq
is the set of sensors which must process the query in
order to give the required answer to the user.

III. SYSTEM ARCHITECTURE

A WSN may contain one or more base stations and hundreds or thousands of sensor nodes. Fig is an example of a WSN. Compared to a base station, a sensor node is very limited in resources. For simplification, we assume that each broadcast message originates from the base station. A sensor node can broadcast messages by first unicasting the message to the base station, which then broadcasts the messages on the sensor node's behalf. In addition, messages transmitted in a sensor network may reach the destination directly or may be forwarded by some intermediate nodes; however, we do not distinguish between them in our scheme. Furthermore, we assume a base station shares a pairwise secret key with each sensor node, allowing each sensor node to securely receive the base station's public key.



Architecture of WSN

IV. CRYPTOGRAPHIC PRIMITIVES

In this section, we introduce various cryptographic primitives and schemes for authentication.

Message Authentication Code
A message authentication code (MAC) is a symmetric cryptographic mechanism that takes as input a k-bit secret key and a message, and outputs an l-bit authentication tag. To exchange authentic messages, a sender and receiver must share the same
secret key. Using the secret key, the sender computes the message's authentication tag (or MAC) and appends it to the message. To verify the authenticity of a message, the receiver computes the message's MAC with the secret key and compares it to the original MAC appended with the message

Collision Resilient Hash Function

A collision-resilient hash function H is a function that maps an arbitrary length message M to a fixed length message digest MD and exhibits the following properties. (1) The description of H is publicly known and does not require any secret information
for its operation. (2) Given x, it is easy to compute H(x). (3) Given y, in the range of H, it is computationally infeasible to find an x such that H(x) = y. (4) It is computationally infeasible to find two distinct messages (M, M') that hash to the same result H(M) =H(M').

Message Authentication Code

A Merkle hash tree can reduce the authentication overhead needed for a large group of data items. For example, a sender signs the root of the tree instead of individual data items. The receiver can then verify the authenticity of every data item by reconstructing the tree and comparing the computed hash value of
the tree, which we call treehash, with the authenticated root value.

Efficiency of Cryptographic Primitives

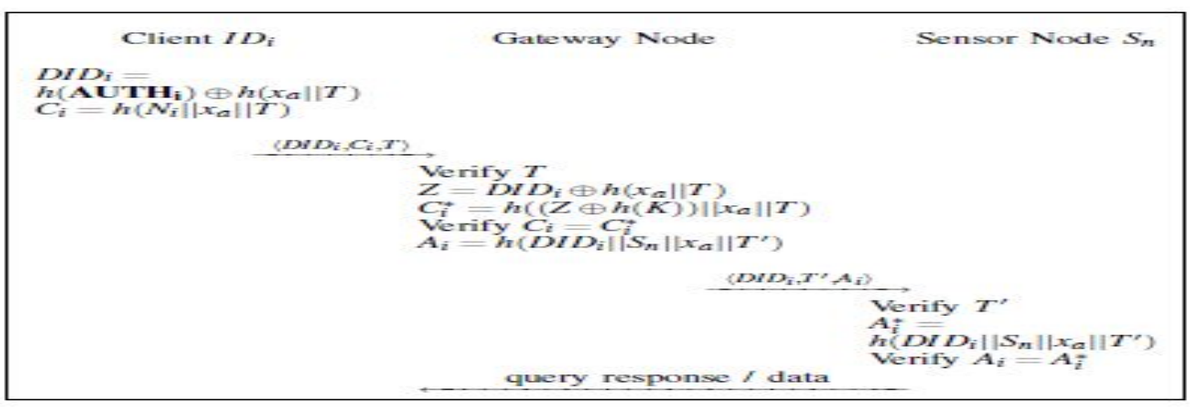
symmetric cryptographic primitives like DES and MD5 are much more efficient than asymmetric
primitives like RSA. The one way hash function is almost as efficient as a symmetric cipher. All experiments are performed on an 8-byte size input, using the OpenSSL libraries on an 800 MHz
Pentium III Linux station.

notation	meaning
GW	identity of gateway node
ID_i	identity of user i
PW_i	password of user i
DID_i	dynamic login identity of user i
S_n	identity of sensor node n
K	symmetric key of the gateway node
x_a	secret parameter
$\oplus$	exclusive OR
$\|\|$	concatenation
$EK_{i,n}$	encryption key of user i and sensor node n
$MK_{i,n}$	MAC key of user i and sensor node n
x_n	symmetric key of sensor node n
$h(m)$	cryptographic hash of m
$h_0(m,k)$	MAC of m using key k
$h_1(s),h_2(s)$	key derivation function with seed s

V. SECURITY CONSIDERATION

A. Password Guessing Attack by Insiders

To be more precise, the password guessing
attack can be implemented as follows:
1) The attacker (say, user j) eavesdrops the victim's (say,user i's) authentication session from which DIDi and T can be extracted.
2) The attacker computes his own DIDj with IDj, PWj, and T, where T is the timestamp from the captured session above.
3) B = h(IDjkPWj) can be prepared because IDj and PWj are the attacker's ID and password, respectively, and his a publicly-known cryptographic hash function.
4) Now the attacker can compute h(IDikPWi) by calculating DIDi_B_DIDj.
5) Now the attacker is ready to mount an off-line password guessing attack with h(IDikPWi). Our patch to the original protocol is to use (IDikPWikxa) instead of h(IDikPWi), which prevents the attacker from completing step 3 because h(IDjkPWjkxa)
requires knowledge of xa hidden in the tamper-proof smart card. The revised protocol uses newly-defined AUTHi and accordingly-modified Ni = (ID‖
jPWj‖xa) _ h(K), which is shown in Fig.



B. Protection of Query Response

It is desirable that a user authentication protocol should be followed by some specific security services such as secure and authentic delivery of sensed data. However, the original protocol in did not care about those security services and omitted the necessary steps such as encryption and authenticity verification of query response. Thus we will add mechanisms that provides those security services by making the gateway node play a role of key distribution center and providing a unique secure channel between a user and a sensor node.

These mechanisms can be realized by establishing a distinct session key for every session and for every pair of a user and a sensor node to frustrate inside attackers and node capturing attackers.

C. Node Compromise Attack

Das claimed that a sensor node must be equipped
with a tamper-proof module to be strong against various attacks caused by node compromise. We show that even with the tamper-proof module, careless implementation of Das's protocol may also cause other security problems such as password guessing attack by outsiders and impersonation of
the gateway node.
_ The tamper-proof module in a sensor node externally
outputs A_i so that the sensor node may compare it withAi.
_ The tamper-proof module does not validate its input properly. For example, it does not check if DIDi and Sn are null or not. Also, it does not examine if the given Sn is the correct ID of the sensor node in which it is installed. In this case, the following attacks are possible.
Password guessing attack
Impersonation of the gateway node.

VI. SECURITY ENHANCED PROTOCOL

We present a security-enhanced two-factor authentication protocol Our authentication protocol is composed of two phases; the registration phase and the authentication phase. The registration
phase is the same as that of Das's protocol except that Ni is computed as Ni = h(IDi‖PWi‖xa)_h(K). The authentication phase begins by user's submitting IDi and PWi to his/her smart card, and the following steps are performed:
1) The user's smart card authenticates IDi and PWi.
2) The smart card computes DIDi = h(IDi‖PWi‖xa) _h(xajjT) and Ci = h(Ni‖xa‖T) to send DIDi;Ci;T to the gateway node.
3) Upon receiving the request from the user, the gateway node validates T and authenticates Ci by comparing it with C_i = h((DIDi_h(xa‖T)_h(K)) ‖xa‖T).
4) The gateway node computes an encryption key
EKi;n = h1(DIDiSn‖(DIDi_h(xa‖T)_h(K)) ‖xa‖T) and a MAC key
8) When Sn receives these data, it first verifies T0 and computesA_i =h0(DIDi‖Sn‖Di‖T0;MKGW;n) using MKGW;n.Then it checks if Ai = A_i .
9) Sn decrypts Di with EKGW;n and recovers EKi;n and MKi;n.
10) Sensed data to be transmitted is encrypted with EKi;n as R=EEKi;n (Data) and a MAC is computed with MKi;n asBi =h0(DIDijjSn‖R‖T00;MKi;n), where T00 is the current time.
11) Sn;R;T00 and Bi are sent to user i.
12) The user verifies T00 and checks Bi by comparing it with B_i = h0(DIDi;Sn;R‖T00;MKi;n), where MKi;n =h2(DIDi‖Sn‖Ni‖xajjT).
13) If this verification is successful, the sensed
data is recovered by decrypting R using
EKi;n = h1(DIDi‖Sn‖Ni‖xa‖T).

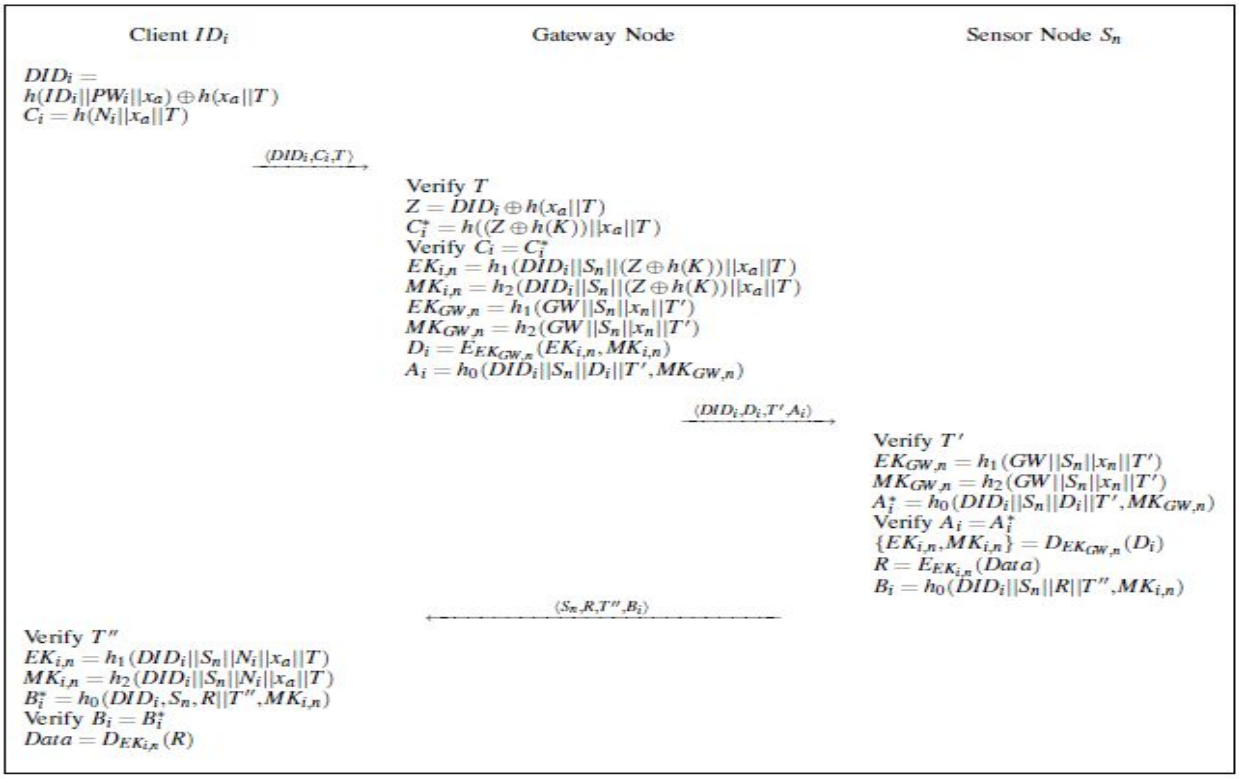
VII. ANALYSIS OF PROPOSED WORK

A) Security analysis

Now we will shows the proposed framework that resists against the following attacks: such as, replay attack,impersonation attack, stolen-verifier attack, password guessing attack, node-compromise attack, man-in-the-middle attack,denial-of-service attack. Furthermore, our framework consider mutual authentication between the GW node and the sensor
node and enable users to change their password freely whenever required.

(B) Performance Analysis

Here we examine the performance and summarize the security functionality of our two-factor framework and compare with the M.L. Das two-factor scheme. Table II shows that our framework is more secure and robust as compares to Das s scheme and provides more security features on reasonable computational costs.



Security enhanced protocol

VIII. CONCLUSION

In this paper, we have proposed an enhanced security protocol user authentication framework for wireless sensor networks, which is imposed on two-factors and using cryptographic hash functions. We have
provided security and performance analysis of the proposed framework

REFERENCES

[1] Li, C.T. Secure smart card based password authentication scheme with user anonymity. Inform. Technol. Contr. **2011**, 40, 157–162.

[2] Li, C.T.; Lee, C.C. A novel user authentication and privacy preserving scheme with smart cards for wireless communications. Math. Comput. Model. **2012**, 55, 35–44.

[3] P. Golle and N. Modadugu, "Authenticating streamed data in the presence of random packet loss," In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2001), pp. 13–22, Internet Society, Feb. 2001. M. Luk, G. Mezzour, A. Perrig and V. Gligor, MiniSec: A Secure Sensor Network Communication Architecture, IPSN 07, April 2007,Cambridge, Massachusetts, USA

[4] C. Karloff, N. Sastry and D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, Proc. of 2nd ACM Conf. on Embedded Networked Sensor System (SenSys 2004), Baltimore, MD, November 2004

[5] M. K. Khan and K. Alghathbar, Cryptanalysis and Security Improvement of Two-Factor User Authentication in Wireless Sensor Networks , Sensors 2010, pp. 2450-2459.

[6] Chan, H., Perrig, A., und Song, D.: Random key predistribution schemes for sensor networks. In: IEEE Symposium on Security and Privacy. S. 197–213. May 2003.