January 2012

User Authentication Techniques for Wireless Sensor Networks : A Survey

Shakera Shaikh

Computer Science & Engineering, G. H. Rasoni College of Engineering, Nagpur, India,
shakera04@gmail.com

Veena Gulhane

Computer Science & Engineering, G. H. Rasoni College of Engineering, Nagpur, India,
vinagulhane@gmail.com

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Shaikh, Shakera and Gulhane, Veena (2012) "User Authentication Techniques for Wireless Sensor Networks : A Survey," *International Journal of Smart Sensor and Adhoc Network*. Vol. 2 : Iss. 2 , Article 2.
DOI: 10.47893/IJSSAN.2012.1142
Available at: <https://www.interscience.in/ijssan/vol2/iss2/2>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

User Authentication Techniques for Wireless Sensor Networks : A Survey

Shakera Shaikh & Veena Gulhane

Computer Science & Engineering, G. H. Raisoni College of Engineering, Nagpur, India
E-mail : shakera04@gmail.com, vinagulhane@gmail.com

Abstract - A wireless sensor network (WSN) consisting of a large number of tiny sensors can be an effective tool for gathering data in diverse kinds of environments. The data collected by each sensor node is communicated to the base station, which forwards the data to the end user. In wireless sensor network data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. This paper synthesizes existing user authentication schemes in wireless sensor networks and highlights the challenges in user authentication.

Keywords - WSNs, data security, authentication.

I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

Sensor Network Security Issue

Two of the most security-oriented applications of wireless sensor networks are military and medical solutions. Due to the nature of the military, it is obvious that the data (sensed or disseminated) is of a private nature and is required to remain this way to ensure the success of the application. Enemy tracking and targeting

are among the most useful applications of wireless sensor networks in military terms.

The choice of which security services to implement on a given sensor mainly depends on the type of application and its security requirements. Amongst these we examined:

- Authenticity - it makes possible that the message receiver is capable of verifying the identity the message sender, hence preventing that likely intruder nodes inject malicious data into the network.
- Confidentiality - it ensures that the content of the message is accessed only by authorized nodes.
- Integrity - it guarantees that should a message have its content modified during the transmission, the receiver is able to identify these alterations.

Security requirement

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

- Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks require configuring the initial duty cycle carefully.
- Authorization, which ensures that only authorized sensors can be involved in providing information to network services.

- Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.
- Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients.
- Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
- Nonrepudiation, which denotes that a node cannot deny sending a message it has previously sent.

Fig. 1 : Wireless sensor Network Scenario

For some special applications of WSNs, such as military surveillance, information gathered is sensitive and must be kept confidential. Therefore in such applications UA is necessary. Health care is a good example of UA application for WSNs: Let's say a WSN offers instantaneous medical data service to subscribed health care employees such as doctors and nurses. Since the confidentiality of the data is important (i.e. patient medical records), only the legitimate users should get a response to their queries. Unauthorized users must be prevented from accessing the mentioned confidential information. Therefore UA is a must in these kinds of networks. UA has been well studied for traditional networks, but those solutions cannot be used for WSNs because of the unique characteristics that WSNs possess.

UA is an intended feature that will increase data security for WSN users and profitability of the network for WSN

II. RELATED WORK

In this section we analyze some popular user Authentication scheme for WSNs.

1) *Public key-based user authentication scheme* [1]

It assume that public key operation is feasible for even a tiny sensor node . All of the public key-based schemes utilize a certificate which is generated by BS and used for user authentication. In general, however, public key operation is slower and consume much more energy than symmetric key operation. Thus, if an attacker launches DOS attack, the attacker can easily exhaust the limited energy of sensor node.

2) *Symmetric key-based user authentication scheme*[2]

A key distribution scheme for dynamic conferences is a method by which initially an (off-line) trusted server distributes private individual pieces of information to a set of users. Later, each member of any group of users of a given size (a dynamic conference) can compute a common secure group key. In this setting, any group of t users can compute a common key by each user computing using only his private initial piece of information and the identities of the other $t - 1$ users in the group. Keys are secure against coalitions of up to k users, that is, even if k users pool together their pieces they cannot compute anything about a key of any t -size conference comprised of other users.

3) *Dynamic user authentication scheme*[3]

It allows legitimate users to query sensor data at any of the sensor nodes in an ad hoc manner. Second, it imposes very little computational load and requires only simple operations. However, their scheme has three security weaknesses, as follows:

- It cannot protect against the replay and forgery attacks.
- Passwords could be revealed by any of the sensor nodes.
- A user cannot change his/her password freely.

4) *A Robust Dynamic User Authentication Scheme* [4]

This scheme can provide protection against the replay attacks of login message as well as accept login message (*Acc_login*). In case of login message, as GW-node checks user ID and timestamp, the adversary node cannot replay it, whereas in case of *Acc_login* message, as a login node checks the authenticator, the adversary node cannot replay it. The proposed scheme provide mutual authentication between login node and gateway node. A gateway node verifies the authenticator containing C_k supplied by the login node while a login node verifies the authenticator containing X furnished by a gateway node.

5) *A lightweight user authentication scheme* [5]

It provides mutual authentication and session-key agreement. The scheme is executed on both sides; the WSN's coordinator side playing the role of the server, and the user's device side acting as a client. It is assumed that there is an administrator, which is responsible for loading necessary secret keys in the WSN and for registration of users. First, the administrator chooses a secret key x and then loads the system server and the coordinator with this secret key x . The system server uses this secret key for registration of users. The coordinator uses this secret key in order to verify the authenticity of users.

6) *An Efficient Scheme for User Authentication in Wireless Sensor Networks* [6]

In this paper, a distributed user authentication scheme suitable for sensor networks based on self-certified keys cryptosystem (SCK) is proposed. First of all, SCK is modified to use the Elliptic Curve Cryptography (ECC) to establish pair-wise keys in sensor networks, because ECC is said to be feasible for WSN even without special hardware support. Secondly, based on these established pair-wise keys, a new efficient user authentication method in sensor networks is given. But this method is vulnerable to node capture attacks and it also requires synchronization between nodes.

7) *Two Tier User Authentication (TTUA) scheme* [3].

In the TTUA scheme, CHs are used as a backbone in the network so that the sensed data, after being collected, are transmitted through CHs towards the requesting users. Between the CHs and the users they issue SKC for authentication. It is practically impossible to scale SKC keys to include a large number of users and sensor nodes, because of the memory limitations. Besides, in SKC excluding existing users from the network and including new users to the network, requires key revoking and key re-distribution, which needs a considerable amount of communication overhead. These are the biggest constraints of the TTUA scheme.

8) *Advanced Two Tier User Authentication (TTUA) scheme* [1]

In this scheme, WSN consists of basically two elements:

1) CHs having high processing capability and long lasting power supplies, such as PDAs. 2) Sensor nodes having low processing capability and limited power supplies, such as MICA2 motes. CHs are assumed as

trusted gateways to the sensor nodes. Hence they have better power supplies compared to sensor nodes, they are more convenient to run power hungry PKC algorithms. Therefore, between CHs and users a PKC algorithm, namely ECC, is used for UA purposes. Once a user is authenticated to a CH, then allowed to access the sensor nodes through that CH. Since it is low power demanding, between CHs and sensor nodes an SKC algorithm is used. WSN consists of CHs and sensor nodes, representing a *Heterogeneous* network structure. ATTUA allows a user to register once and authenticate to the network many times. Users can also change the password anytime at will. We consider wide scale WSN deployed in any variety of environments. In our WSN's architecture, base station (BS) is the point of central control, which serves as a trusted key management facility. BS is many orders of magnitude more powerful than sensor nodes. Typically, BSs have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, stronger processors, and means for communicating with outside networks. After the deployment, sensor nodes form groups, called clusters. For each cluster, a powerful node is assigned as a CH. CHs have higher communication power than sensor nodes and therefore possess far more radio transmission coverage. CHs can communicate with each other and also with BS. In order to protect the keying materials, CHs are equipped with tamper-resistant hardware. This assumption is reasonable, hence the number of CHs in a heterogeneous WSN is relatively small (e.g., approximately 20-30 CHs for 1,000 sensors), and the cost of such tamper-resistant hardware is small [6]. Users are equipped with portable computing devices, such as laptops, with no power constraints compared to sensor nodes. Users interact with the WSN for data query and retrieval. After processing sensed information, the sensor node either sends the data upon event detection or stores it to serve for the next query.

III. COMPARISON OF USER AUTHENTICATION SCHEMES

Table 1 summarizes the authentication Techniques surveyed in this paper.

Scheme	Authentication	Scalability	Communication cost	Communication speed
ESUAS	Unilateral	No	High	Less
IDUAS	Unilateral	Yes	High	Less
RDUAS	Mutual	No	High	Less
LUAS	Mutual	Yes	High	Less
ATTUA	Unilateral	Yes	Less	Less

IV. CONCLUSION

For some special applications of WSNs, such as military surveillance, information gathered is sensitive and must be kept confidential. Therefore in such applications UA is necessary. There Exist a Large number of user authentication techniques and some are reviewed in this paper. The focus in all the paper is only on security, however scalability, communication cost is high and communication speed is less due to more computational load. Compelling challenges for authentication techniques are how to increase scalability of the network, communication speed and how to decrease communication cost in order to provide security in less time.

REFERENCES

- [1] Ismail Butun and Ravi Sankar,2011.” Advanced Two Tier User Authentication Scheme for Heterogeneous Wireless Sensor Networks”. 2nd IEEE CCNC Research Student Workshop.
- [2] X.H. Le, S. Lee, and Y.K. Lee. ”Two-Tier User Authentication Scheme for Heterogeneous Sensor Networks.” the 5th IEEE International Conference on Distributed Computing in Sensor Systems, (DCOSS '09), Marina Del Rey, California, USA, June 8-10, 2009.
- [3] K.H.M. Wong, Y. Zheng, J. Cao, and S. Wang. ”A dynamic user authentication scheme for wireless sensor networks.” IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006.
- [4] Binod Vaidya, Jorge Sá Silva, Joel J. P. C. Rodrigues,2009.” Robust Dynamic User Authentication Scheme for Wireless Sensor Networks”proceeding of the 5th ACM symposium on QOS and security for wireless and mobile networks.
- [5] Omar Cheikhrouhou^{1,2}, Anis Koubaa^{3,4}, Manel Boujelben¹, Mohamed Abid¹,2010.” A Lightweight User Authentication Scheme forWireless Sensor Networks” International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.
- [6] C. Jiang, B. Li, and H. Xu, “An efficient scheme for user authentication in wireless sensor networks” in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007
- [7] X. Du, G. Mohsen, X.O. Yang, C. Hsiao-Hwa. ”Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks.” IEEE Transactions on Wireless Communications, Vol.6 (9), September 2007, pp. 3395-3401.