A User Authentication Scheme with Privacy Protection for Wireless Sensor Networks *

Sungjune Yoon, Hyunrok Lee, Sungbae Ji, and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University (ICU), Korea
{pridekk, tank, grail, kkj}@icu.ac.kr

Abstract. In wireless sensor networks, user authentication is a wireless mutual authentication process between a user and sensor nodes by which people could acquire the environmental information around them. It is really necessary because in the upcoming ubiquitous age, people will want to utilize this information for enhancing their daily activities. Since a sensor node has very limited resources, we want to provide the information only to legitimate users in order to conserve the small power consumption. For this purpose, sensor node must verify the user in an efficient and secure manner. In addition, we must protect the privacy of the user because all messages are broadcasted on the air which means that an attacker can easily infringe the privacy of the user by eavesdropping the broadcasted messages. In this paper, we propose an efficient and secure user authentication scheme which utilizes the local time of each sensor nodes and protects the privacy of user.

Keywords: Wireless sensor networks, user authentication, privacy

1 Introduction

Wireless sensor network (*WSN*) has been gaining a lot of interest as one of the core techniques for the upcoming ubiquitous age. A *WSN* is an *ad-hoc* network of a large number of sensor nodes which collect environmental data. Since the data is broadcasted on the air and sensor nodes are vulnerable to many attacks such as node capture attacks and *DOS* attacks, countermeasures are inevitably necessary for defending against these attacks. Up to now, researchers have proposed many security mechanisms for protecting *WSN* from these types of attacks. As a result, there are many protocols [4, 6, 9–12, 14, 16, 18] that defend *WSN* against such malicious attacks. Furthermore, some researchers have proposed user authentication schemes by which sensor nodes can directly provide valuable information only to legitimate users [5, 8, 13, 17, 19, 20].

To acquire environmental information gathered by sensor nodes, a user will carry a mobile device, such as a mobile phone, a PDA, or a laptop computer.

* This work was supported by the IT R&D program of MIC/IITA. [2005-S-106-02, Development of Sensor Tag and Sensor Node Technologies for RFID/USN]

Before collecting the information from sensor nodes, this device should verify the user via password or biometric information. After authenticating the user, the device should proceed to an authentication process with its local sensor nodes so that the device can collect the environmental information. From now on, we name this device User Agent (UA). Fig. 1 shows the relationship between UA and *WSN*.

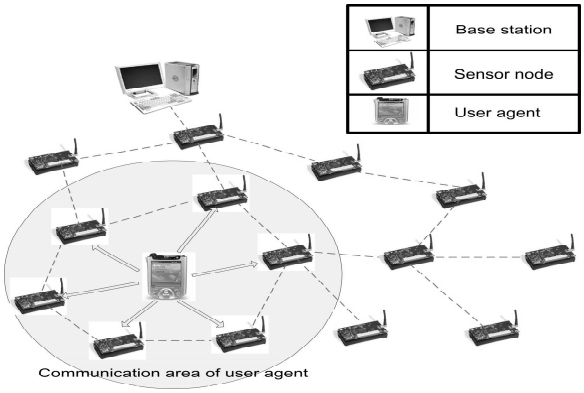

Fig. 1. User agent and wireless sensor network

In general, UA can directly communicate with BS through existing mobile communication system. For example, a mobile phone is able to access the Internet almost everywhere. In this case, the mobile phone can send its current position to BS and then the BS directly provides the environmental information to the mobile phone, but it has the following problems:

- Firstly, if the data produced by sensor nodes is intermittently collected by the BS, then this information provided by the BS may not be up-to-date.
- Secondly, in order to provide fresh data to user, the BS has to broadcast queries which are targeted to the user's local sensor nodes. This expends the energy of the other nodes which relay these queries.

In order to solve these problems, user needs a means to directly communicate with sensor nodes and before beginning this communication, sensor nodes must authenticate the user and observe activities of the user to protect themselves from malicious attacks. In addition, a user authentication scheme must conceal the information of the user during the authentication process. If the information is revealed in the authentication step, it could violate user privacy. An attacker, for example, can easily monitor the whereabouts of the users by eavesdropping authentication messages.

In *WSN*, user authentication schemes are classified into two categories: public key-based user authentication [5, 8, 19, 20] and symmetric key-based user authentication [13, 17]. Public key-based user authentication schemes assume that

public key operation is feasible for even a tiny sensor node [15]. 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. Many symmetric key-based user authentication schemes adopt Blundo scheme [2], which is a key pre-distribution scheme. Although these schemes are more efficient than the public key-based schemes, they also have some problems: once authenticated, always authenticated [13]; the trajectory of a user must be predetermined [17].

In addition, all the above mentioned schemes could violate user privacy, because they reveal the ID of a user [8, 13, 19, 20] and only consider the characteristics of sensor node and the computing power of UA, but do not consider the other abilities of UA. Moreover, most schemes assumed that WSN has a time synchronization mechanism by which they create a certificate [5, 8, 19, 20] or a pair-wise key [17]. Since time synchronization consistently consumes the limited energy of sensor nodes, a scheme is more efficient and reliable than others if the scheme does not depend on any time synchronization protocol.

In this paper, we propose an efficient and secure user authentication scheme which protects the privacy of the user and utilizes the local time clock of sensor nodes and additional advantages of the user, *i.e.* the communication ability as well as the computation power of UA. The merits of our scheme are as follows:

1. It reduces the energy consumption of sensor nodes as it does not need any public key operation.
2. It does not require any time synchronization mechanism.
3. It protects the privacy of the user.

The remaining part of this paper is organized as follows: In Section 2, we briefly review the related work on the user authentication for WSN. In Section 3, we describe our goal and assumption. In Sections 4 and 5, we propose a secure and efficient user authentication scheme with privacy protection and analyze its cryptographic strength, respectively. Finally, we make a conclusion in Section 6.

2 Related Work

In [19, 20], Benenson *et al.* uses a public key-based certificate for verifying the source of a query, under the assumption that public key operation is viable even in the resource-constrained sensor nodes. However, public key operation is much slower than symmetric key operation; while launching a DOS attack, an attacker can easily exhaust the limited energy of sensor node. Wong *et al.* [8] and Wang and Li [5] proposed user authentication schemes, which exhibit the same weakness as mentioned above, because they also used public key operation in their schemes. Banerjee and Mukhopadhyay [13] applied a random polynomial key pre-distribution scheme [2] to UA for verifying its legitimacy, but did not

consider the "UA capture attack," *i.e.*, when a UA is compromised, an attacker can get all the information from any sensor node at anytime.

Although Zhang *et al.* [17] have proposed a user authentication scheme that is resilient against the UA capture attack, the trajectory of user has to be predetermined in their scheme. It is suitable for network management (in this case, BS can predict the trajectory of UA), but inadequate for normal user whose trajectory is difficult to predict. Moreover, all the above mentioned schemes reveal the information of the user where the ID of the user is broadcasted in an unencrypted form. Since an attacker can easily eavesdrop on the broadcasted ID, the attacker can track the whereabouts of the user. It could violate the privacy of the user.

3 Preliminaries

In this section, we explain our design goal and the basic assumption regarding *WSN*, *UA*, and the user.

3.1 Design Goal

Our goal is to design a user authentication scheme to reduce potential problems caused by illegitimate users and compromised sensor nodes; thus protecting honest sensor nodes from *DOS* attacks and user privacy from compromised sensor nodes. In addition, we will propose a user authentication scheme to satisfy the following requirements:

- **Privacy protection**: If the ID of a user is revealed after user authentication process, it will violate user privacy because every sensor node is vulnerable to "node capture attack" by which an attacker can easily track the movement of the user.
- **Lightweight**: Typical sensor nodes such as Telosb or MicaZ [3] have very limited resources and limited energy. Therefore, the scheme must be efficient in terms of communication and computation in order to reduce the energy consumption of sensor node.
- **Access control**: If sensor nodes process all the requests from legitimate users, it could even process erroneous requests that users may not intend or be allowed to query. Since it could deprive sensor node of its limited energy, the sensor node must always check the access control rights of the user.

3.2 Assumption

WSN is considered to be an *ad-hoc* network which consists of a large number of sensor nodes and few base stations. Each sensor node can be either automatically configured into a network or not, since some of sensor nodes could be intermittently disconnected with the network due to their environmental condition. We do not consider time synchronization because it constantly consumes the limited energy of all the sensor nodes in the network.

– **Sensor node**: Each sensor node continuously collects environmental data such as temperature, humidity, seismicity, *etc* and provides the data only to legitimate user. It means that sensor node must verify the source of the request. We assume that every sensor node has limited resources and limited energy source and has an internal clock. Some examples are Telosb and MicaZ [3]. Symmetric key operation is much more efficient and faster than any of public key operation and does not affect the life time of a sensor node.
– **Base Station** (BS): It is a device which collects the information provided by sensor node and manages *WSN*. It is always trusted by all the sensor nodes and users and must be secured against any type of attacks. It helps user and sensor node to authenticate each other by generating a ticket which includes a pair-wise key between a user and a sensor node, its expiration time, an access control list of the user, *etc*.

User is a person who wants to utilize the information of his or her local sensor nodes in order to make his or her everyday life much more comfortable than before. The user has a mobile device which is able to communicate with *WSN*. We call this mobile device as user agent. Before the user agent proceeds to a user authentication process with its local sensor nodes, it must authenticate the user via password or biometric information.

User agent (UA) is a mobile device, such as a mobile phone or a PDA with a radio module able to communicate with sensor nodes. It can communicate with sensor nodes only after authenticating its owner, first. We assume that mobile phone can communicate with BS directly through its mobile network and PDA can do it via its *WLAN*. This assumption is acceptable because these kinds of networks are now widely used in the world. Therefore, We assume that a secure *out-of-band* channel is established between UA and BS before starting user authentication processes between the UA and its local sensor nodes.

4 Our proposed scheme

In this section, we describe our proposed scheme. At first, we define our notations used in the rest of this paper summarized in Table 1. We adopt Kerberos [7] which provides both entity authentication and key establishment using symmetric key-based encryption techniques and a third party [1] and remodel it to be suitable for our assumption since it reveals the ID of user and heavily depends on time synchronization.

1. The UA generates a random number, R_{UA}, and hashes its ID concatenated with the random number. Then, the UA broadcasts the hashed value.

$$UA \rightarrow N_i{:}h(ID_{UA}||R_{UA}) \tag{1}$$

Table 1. Notations

Notation	Description
BS	A base station
UA	A user agent
N_i	i^{th} sensor node
ID_U	Identity of U
$K_{A,B}$	Shared secret key between entities A and B
T_{N_i}	Current time of N_i (local time stamp)
R_U	A random number generated by U
AL_{UA}	The access control list of UA
$Ticket$	A ticket generated by BS
t_e	Expiration time
$M_1 \| \| M_2$	Concatenation between messages M_1 and M_2
$h()$	A hash function
$E_{K_{a,b}}()$	Symmetric encryption with a key, $K_{A,B}$
$\rightarrow$	A secure communication channel
$\Rightarrow$	An insecure communication channel
$A \rightarrow B : C$	C is transferred from A to B via the insecure channel
$A \Rightarrow B : C$	C is transferred from A to B via the secure channel

2. On receiving *Eq.*(1), each sensor node encrypts its local time and the received value using K_{BS,N_i} and then sends the encrypted value with its ID_{N_i} to the UA.

$$N_i \rightarrow UA{:}ID_{N_i}||E_{K_{BS,N_i}}(T_{N_i}||h(ID_{UA}||R_{UA})) \tag{2}$$

3. The UA sends R_{UA} and *Eq.*(2) to the BS through the secure channel.

$$UA \Rightarrow BS{:}R_{UA}||ID_{N_i}||E_{K_{BS,N_i}}(T_{N_i}||h(ID_{UA}||R_{UA})) \tag{3}$$

4. The BS decrypts $E_{K_{BS,N_i}}(T_{N_i}||h(ID_{UA}||R_{UA}))$ and hashes ID_{UA}, which the BS have already known in our assumption, concatenated with R_{UA} and then compares it with the decrypted message. If the values are equal, the BS generates a ticket based on T_{N_i}, the right of the user, and then sends the ticket to the UA.

$$BS \Rightarrow UA{:}ID_{N_i}||T_{N_i}||T_{N_i}+t_e||AL_{UA}||K_{UA,N_i}||Ticket \tag{4}$$

$$Ticket{=}E_{K_{BS,N_i}}(h(ID_{UA}||R_{UA})||T_{N_i}||T_{N_i}+t_e||AL_{UA}||K_{UA,N_i}) \tag{5}$$

5. The UA generates a random number, R'_{UA}, and encrypts it using K_{UA,N_i}. Then, the UA sends it with the ticket to the sensor node, N_i.

$$UA \rightarrow N_i{:}E_{K_{UA,N_i}}(R'_{UA})||Ticket \tag{6}$$

6. The N_i authenticates the UA after verifying the received ticket and decrypts $E_{K_{UA,N_i}}(R'_{UA})$ using K_{UA,N_i}. After that, the N_i encrypts $R'_{UA}+1$ using K_{UA,N_i} and sends it to the UA.

$$N_i \rightarrow UA{:}E_{K_{UA,N_i}}(R'_{UA}+1) \tag{7}$$

On receiving *Eq.*(7), the UA verifies whether the N_i knows the shared secret, K_{UA,N_i}, or not. If the verification is successfully finished, the UA can request information from N_i in the period between T_n and T_n+t_e using the key, K_{UA,N_i}. Fig. 2 shows the overall scheme.

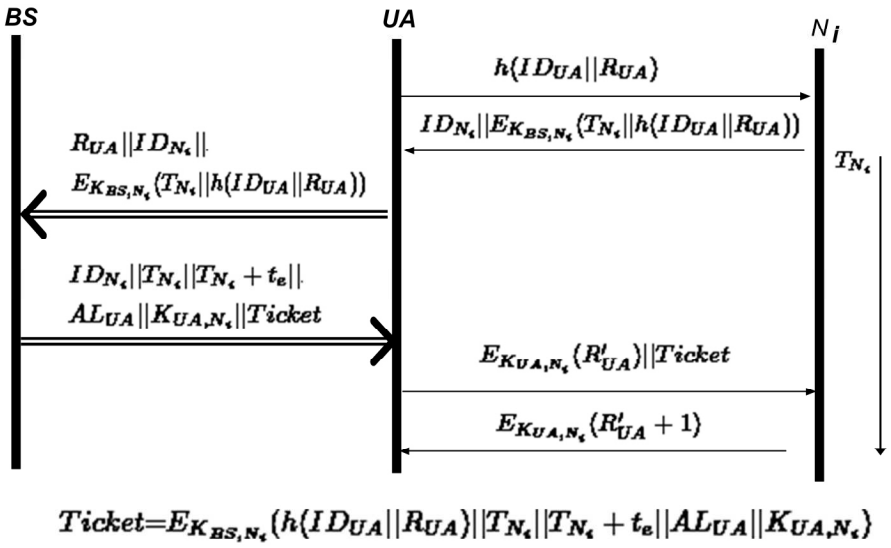

Fig. 2. The Proposed Scheme

5 Analysis

The proposed scheme is similar to the Kerberos protocol. For its proper operation, however, Kerberos heavily depends on the *network-wide* time synchronization which is acceptable in the typical distributed computing environment, but not in *WSN* as it consists of a large number of resource-constrained sensor nodes. Our scheme does not depend on the time synchronization because it uses the local time stamp of sensor node to which the UA wants to authenticate itself. Table. 2 shows the comparison with other schemes.

Table 2. Comparison with other schemes

Scheme	Benenson *et al.*[20]	Wang and Li [5]	Zhang *et al.* [17]	Our scheme
Sensor node operation cost	$2PK$	$2H+1SK+3PK$	$1H$	$4SK$
Privacy protection	No	No	No	Yes
User trajectory	Random	Random	Predetermined	Random
Time synchronization	Needed	Needed	Needed	Not Needed

PK: Public key operation SK: Symmetric key operation H: Hash operation

5.1 Mutual authentication

The BS is a third party trusted by both UA and sensor node. For user authentication, it issues a ticket according to the ID of the user, ID_{UA}, and the sensor node, N_i. Since only legitimate user can request a ticket and legitimate sensor node can share a secret with the BS, both the user and the sensor node authenticate each other according to the ticket in the authentication steps *Eq.*(6) and *Eq.*(7). Even if an attacker compromise a few number of sensor nodes, it does not damage any others authentication processes.

5.2 Privacy protection

Most previous works do not consider the privacy of the user, but it must be deliberated. Since all messages are broadcasted on the air in *WSN*, an attacker can easily eavesdrop the messages. It can violate user privacy such as monitoring the whereabouts of the user. To protect the user privacy in our scheme, the ID of user is always hashed with a random number, $H(ID||R)$, for hiding the ID before broadcasting. Receiving the broadcasted hashed value, the sensor node, N_i, starts to verify the user. Even after finishing the user authentication, the sensor node does not know who the user is because it identifies the user with the hash value, *i.e.*, none of the sensor nodes know the real ID of the user. This prevents user privacy violation.

5.3 Efficiency

Our proposed scheme only uses four symmetric key operations in a sensor node. Since symmetric key operation is generally much faster and more efficient than any public key operation, it reduces the energy consumption of sensor nodes.

5.4 Access control

A sensor node processes a request of a legitimate user only if the request is allowed to the user based on the access control list of the user, AL_{UA}. It protects the sensor node from careless queries of the legitimate user and conserves the energy of the sensor node.

5.5 No time synchronization

Kerberos and other authentication schemes that we mentioned before heavily depend on time synchronization. In *WSN*, the time synchronization continuously consumes the limited energy of all the sensor nodes. Even more, if an attacker destroys some parts of WSN, the time synchronization will be not provided for a while. In this case, Kerberos and other schemes are not operated properly, but our scheme is not affected. Our scheme does not need any time synchronization protocol at all because it creates tickets based on the local time stamp, T_{N_i}, of the sensor node, N_i. Thus, our scheme can conserve the limited energy of sensor node and continue to operate even when the network configuration is disintegrated.

6 Conclusion

In the upcoming ubiquitous era, the user will want to easily and securely acquire the environmental information in their local area, but at the same time, the ubiquitous environment will want to provides its data only to legitimate users. For this purpose, mutual authentication between the user and the environment must be provided. In this paper, we propose a secure and efficient user authentication scheme, which safeguards the privacy of the user and mutually authenticates UA and sensor node without any need for time synchronization scheme. Even if some parts of *WSN* are not synchronized, user and sensor node can easily authenticate each other since our scheme does not depend on the time synchronization, but only need the internal clock counter (*i.e.*, local time stamp) of each sensor node. Furthermore, our scheme provides a privacy protection mechanism using a hash function. In the future, we will apply our scheme to the real environment and measure the exact resources and energy consumption.

References

1. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
2. Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung, Perfectly-Secure Key Distribution for Dynamic Conferences, In *Advances in Cryptology, Proceedings of CRYPTO92*, LNCS 740, pp. 471-486, 1993.
3. Crossbow, Inc. http://www.xbow.com/.

4. D. Braginsky and D. Estrin, Rumor Routing Algorthim for Sensor Networks, In *Proceedings of the first ACM International Workshop on Wireless Sensor Networks and Applications (WSNA)*, September 2002.
5. Haodong Wang and Qun Li, Distributed User Access Control in Sensor Networks, In *Proceedings of the Second IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, June 2006.
6. H. Chan and A. Perrig, PIKE: Peer Intermediaries for Key Establishment in Sensor Networks, In *the Twenty Forth Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom)*, March 2005.
7. J. T. Kohl and B. C. Neuman, The Kerberos Network Authentication Service (Version 5), Internet Engineering Task Force, Networking Group, Internet Draft RFC 1510, September 1993.
8. Kirk H.M. Wong, Yuan Zheng, Jiannong Cao, and Shengwei Wang, Dynamic User Authentication Scheme for Wireless Sensor Networks, *In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, June 2006.
9. L. Eschenauer and V. D. Gligor, A Key-Management Scheme for Distributed Sensor Networks, In *Proceedings of the Ninth ACM Conference on Computer and Communications Security (CCS)*, November 2002.
10. L. Hu and D. Evans, Secure Aggregation for Wireless Networks, In *Proceedings of the 2003 IEEE Symposium on Applications and the Internet Workshops (SAINT)*, January 2003.
11. N. Shrivastava, C. Buragohain, D. Agrawal, and S. Suri, Medians and Beyond: New Aggregation Techniques for Sensor Networks, In *Proceedings of the Second ACM International Conference on Embedded Networked Sensor Systems (SenSys)*, November 2004.
12. Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang. Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks, In *Proceedings of the Second ACM International Conference on Wireless Sensor Networks and Applications (WSNA)*, September 2003.
13. Satyajit Banerjee and Debapriyay Mukhopadhyay, Symmetric Key Based Authenticated Querying in Wireless Sensor Networks, In *Proceedings of the First ACM International Conference on Integrated Internet Ad hoc and Sensor Networks (InterSense)*, May 2006.
14. S. Ganeriwal and M. Srivastava, Reputation-based Framework for High Integrity Sensor Networks, In *Proceedings of the Second ACM Workshop on Security of Ad hoc and Sensor Networks (SASN)*, October 2004.
15. V. Gupta, M. Millard, S. Fung, Y. Zhu, N. Gura, H. Eberle, and S. C. Shantz, Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet, In *the Third IEEE International Conference on Pervasive Computing and Communication (PerCom)*, March 2005.
16. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks, In *Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS)*, October 2003.
17. Wensheng Zhang, Hui Song, Sencun Zhu, and Guohong Cao, Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks, In *the Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, May 2005.
18. Y. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, In *the Twenty Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2003.

19. Z. Benenson, Authenticated Queries in Sensor Networks, In *the Second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, July 2005.
20. Z. Benenson, N. Gedicke, and O. Raivio, Realizing Robust User Authentication in Sensor Networks, In *Proceedings of the First Workshop on Real-World Wireless Sensor Networks (REALWSN)*, June 2005.