IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Remote User Authentication in WSN using ABCRNG

D. Thamaraiselvi[1], Dr. M. Ramakrishnan[2]

Asst. Professor, CSE Department, SCSVMV University, Kanchipuram, India [1]

Professor, IT Department, Madurai Kamarajar, University, Madurai, India [2]

Abstract: Authenticating a user is very important in un attended environment like wireless sensor network. Wireless sensor networks are used to monitor physical or environmental conditions. Authenticating a user in wireless sensor networks is more difficult than in traditional networks owing to sensor network characteristics such as unreliable communication networks, resource limitation, and unattended operation. As a result, various authentication schemes have been proposed to provide secure and efficient communication. In this proposed paper id based remote user authentication is proposed, where the id is generated by using ABCRNG.

Keywords: Authentication, ABCRNG, Wireless sensor networks, public key cryptography, random number.

I. INTRODUCTION

A wireless sensor networks consist of a set of nodes deployed in large numbers to collect and transmit environmental data to a collection point named Base Station (BS).These networks have a particular interest for military applications, environmental, home automation, medical, and many of the applications related to the monitoring of critical infrastructures. A user can access to the collected data either directly or remotely [1].

In the first case, user with mobile device communicates directly with the sensor nodes. For security reasons, access to the sensor networks should be controlled. So to protect the network from various attacks we proposed an authentication solution for this mobile user. We take into consideration that authenticating remote users in WSNs is an important security issue due to their unattended and hostile deployments. Moreover, sensor nodes are usually equipped with limited computing power, storage, and communication modules.

Thus, authenticating remote user in such resource-constrained environment is a challenge security concern. In this paper, we propose a user authentication scheme based on ID generated by ABCRNG which provide authentication and key agreement. We can conceive, for example, a WSN deployed by a commercial company over a large geographical area to capture the physical phenomena of the environment such as temperature, humidity, etc.

Accessing this data will, in general, not be for free since the deployment of a WSN induces some costs. This means that the deployment agencies of some of these services will make them available only to subscribers. In this case, a WSN must be able to distinguish legitimate users from illegitimate ones, resulting in the problem of access control.

The customer of this company must pass an authentication protocol for each new session and take data according to his privileges described in the database system. users in such resource-constrained environment is a challenge security concern.

In this paper, we propose a user authentication scheme based on ID generated by ABCRNG. It provides authentication and key agreement. We can conceive, for example, a WSN deployed by a commercial company over a large geographical area to capture the physical phenomena of the environment such as temperature, humidity, etc. Accessing this data will, in general, not be for free since the deployment of a WSN induces some costs. This means that the deployment agencies of some of these services will make them available only to subscribers. In this case, a WSN must be able to distinguish legitimate users from illegitimate ones, resulting in the problem of access control. The customer of this company must pass an authentication protocol for each new session and take data according to his privileges described in the database system.

II. RELATED WORK

Although, user authentication in e-commerce and m-commerce application is deeply addressed, the problem of user authentication in WSNs was firstly identified, only in 2004, by Benenson et al. [6]. The latter proposes a user authentication scheme based on public key cryptography and which addresses the problem of node capture attacks [7].The scheme prevents unauthorized user from accessing data collected by sensor nodes even in presence of node capture attacks. The scheme is t-out-n, i.e. as the number of compromised node is less than t (where t<n, and n: number of nodes in the communication range of the user) it is still secured. However, the scheme presents some drawbacks as follows. First, it requires that each pair of nodes share a

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

secret key which leads to high storage space and suffers from the problem of scalability. Second, the scheme allows the process of query only by one node. This node must be identified by the node in proximity of user. How to identify the target node is not presented in Benenson et al.'s solution. This process necessary requires that each node has knowledge of the entire network. Third, the scheme doesn't address the case where the node responsible of processing the query is compromised and thus can send fault information.

Banerjee et al. [8] proposed a symmetric key based user authentication scheme. Contrary to Benenson et al.'s scheme, in their solution all nodes reply to the user's query. The scheme is based on Blundo et al.'s techniques [9] for sharing pair-wise key. Sensors involved in user's query generate nonce and user must compute a valid MAC of this generated nonce. Sensor receiving a valid MAC reply to user otherwise it drops the request.

However, Banerjee et al. didn't mention how to determine sensor involved in the user's query. In addition the scheme is vulnerable to node compromise and it doesn't provide mutual authentication. Jiang et al. [10] proposed also a distributed user authentication scheme based on the self-certified keys cryptosystem (SCK) which they modified to use ECC.

Local nodes act collaboratively to determine whether a user has the authorization to access the sensor network. The weakness of this scheme is that each node receiving this access request from a user, must compute a pairwise key, shared with this user and an encrypted nonce using ECC what is an expensive operation to the small local node.

All the precedent schemes are described in the traditional sensors networks. Recently, Rong FAN et al. design a solution for user authentication in two tiered architecture for WSNs [14], in this protocol user authenticate with the gateway node to get access only to nodes in its cell. However, authors do not mentioned in this paper any protocol of updating the data table from user, in this case, the user will be rejected by the GW even if it is a legitimate user.

It is a cumbersome method especially for a large number of users to modify the content of their smart card to each change in network topology. This protocol requires that the three entity user, master node and sensor node must be synchronized between them to achieve the authentication process successfully and to avoid the replay attack but it is well known that the physical clocks of several devices that operate in a distributed system cannot be perfectly synchronized. This causes problems when we want to calculate the time taken by a message during its transfer from one node to another.

III. OVERVIEW OF ABCRNG

3.1 Artificial bee colony algorithm (ABCRNG)

ABC is a new swarm intelligence algorithm proposed by Karaboga in 2005[7], which is inspired by the behavior of honey bees. Since the development of ABC, it has been applied to solve different kinds of problems.

ABC algorithm consists of three kinds of bees namely employed bees, onlooker bees and scout bees. An employed bee forms half of the colony, and the rest includes onlooker bees. Employed bees are in charge of exploiting the nectar sources explored before and giving information to the waiting bees (onlooker bees) in the hive about the quality of the food source sites which they are exploiting. Onlooker bees stay in the hive and decide on a food source to exploit based on the information shared by the employed bees. Scouts search the environment randomly in order to find a new food source depending on an internal motivation or based on possible external clues. This evolving intelligent performance in foraging bees can be represented as follows:

i. At the initial phase of the foraging process, the bees randomly initiate to explore the environment in order to find a food source.
ii. The bee becomes an employed forager after finding a food source. Then it starts to exploit the discovered source. The employed bee returns to the hive with the nectar and unloads the nectar. After unloading the nectar, she can go back to her discovered source site directly or she can share information about her source site by performing a dance on the dance area. If her source is exhausted, she becomes a scout and starts to randomly search for a new source.
iii. Onlooker bees waiting in the hive watch the dances advertising the profitable sources and choose a source site depending on the frequency of a dance proportional to the quality of the source.

In the ABC algorithm proposed by Karaboga [7], the position of a food source represents a possible solution to the optimization problem, and the nectar amount of a food source corresponds to the profitability (fitness) of the associated solution. Each food source is exploited by only one employed bee. In other words, the number of employed bees is equal to the number of food sources existing around the hive (number of solutions in the population). The employed bee whose food source has been abandoned becomes a scout.

3.2.1. Producing initial food source sites

If the search space is considered to be the environment of the hive that contains the food source sites, the algorithm starts with randomly producing food source sites that correspond to the solutions in the search space. Initial food sources are produced randomly within the range of the boundaries of the parameters. Xij=Xjmin+rand (0, 1) (Xjmax-XjMin), where i = 1. . .SN, j = 1. . .D. (1) SN is the number of food sources and D is the number of optimization parameters Equation (1). In addition, counters which store the numbers of trials of solutions are reset to 0 in this phase.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

After initialization, the population of the food sources (solutions) is subjected to repeat cycles of the search processes of the employed bees, the onlooker bees and the scout bees. Termination criteria for the ABC algorithm might be reaching a maximum cycle number (MCN) or meeting an error tolerance

3.2.2. Sending employed bees to the food source sites

As mentioned earlier, each employed bee is associated with only one food source site. Hence, the number of food source sites is equal to the number of employed bees. An employed bee produces a modification on the position of the food source (solution) in her memory depending on local information (visual information) and finds a neighboring food source, and then evaluates its quality. In ABC, finding a neighboring food source is defined by Eq. (2)

$$Vij=Xij+\varnothing ij(Xij-Xj)$$

Within the neighbourhood of every food source site represented by x_i, a food source t_i is determined by changing one parameter of x_i. In Eq. (2), j is a random integer in the range [1, D] and kϵ{1,2, . . .SN} is a randomly chosen index that has to be different from i.ϕ_{ij} is a uniformly distributed real random number in the range [-1,1].

As can be seen from Eq. (2), as the difference between the parameters of the $x_{i,j}$ and $x_{k,j}$ decreases, the perturbation on the position $x_{i,j}$ decreases. Thus, as the search approaches to the optimal solution in the search space, the step length is adaptively reduced.

If a parameter value produced by this operation exceeds its predetermined boundaries, the parameter can be set to an acceptable value. In this work, the value of the parameter exceeding its boundary is set to its boundaries.

After producing v_i within the boundaries, a fitness value for a minimization problem can be assigned to the solution v_i by Eq. (3).

$$\textbf{Fitness}_i= \begin{cases} \frac{1}{1+f_i} & if\ f_i \geq 0 \\ 1+abs(f_i) & if\ f_i < 0 \end{cases} \quad (3)$$

where f_i is the cost value of the solution t_i. For maximization problems, the cost function can be directly used as a fitness function. A greedy selection is applied between x_i and t_i; then the better one is selected depending on fitness values representing the nectar amount of the food sources at x_i and t_i. If the source at t_i is superior to that of x_i in terms of profitability, the employed bee memorizes the new position and forgets the old one. Otherwise the previous position is kept in memory. If x_i cannot be improved, its counter holding the number of trials is incremented by 1, otherwise, the counter is reset to 0.

3.2.3. Calculating probability values involved in probabilistic selection

After all employed bees complete their searches, they share their information related to the nectar amounts and the positions of their sources with the onlooker bees on the dance area. This is the multiple interaction features of the artificial bees of ABC. An onlooker bee evaluates the nectar information taken from all employed bees and chooses a food source site with a probability related to its nectar amount. This probabilistic selection depends on the fitness values of the solutions in the population.

A fitness-based selection scheme might be a roulette wheel, ranking based, stochastic universal sampling, tournament selection or another selection scheme. In basic ABC, roulette wheel selection scheme in which each slice is proportional in size to the fitness value is employed Eq. (4)

$$\textbf{P}_i=\textbf{fitness}_i \qquad (4)$$

In this probabilistic selection scheme, as the nectar amount of food sources (the fitness of solutions) increases, the number of onlookers visiting them increases, too. This is the positive feedback feature of ABC illustrated in the Fig.1.ABCRNG

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

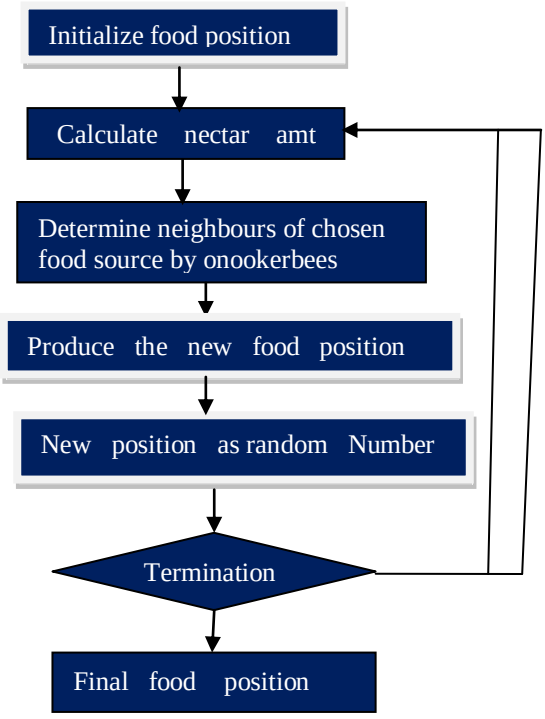

Fig1: flow of ABCRNG

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

IV. THE PROPOSED SCHEME

The proposed scheme provides the mutual authentication and a session key agreement between a user U and a remote gateways node. This protocol is divided into three phases: system initialization phase, user registration phase, and mutual authentication with key agreement phase.

A. System initialization phase:

Step1. The server chooses an (a , b) with order n and a base point P with the order n over $E_p(a, b)$, where n is a large number for the security considerations.

Step2. The server S selects:

- A secret key X_{BS} : used in generating the authentication keys of users ,
- A public key $Y_{BS} \square X_{BS} \square P$,
- A secret key Z and offers it to all users and gateways node: this key is used to the first step of authentication.

Step3. Before deployment, the BS provides to each Gateway nodes a secret key X_{GW} and a public key Y_{GW}.

Step4. The server chooses a secure one-way hash functions, HMAC function, Encrypt and Decrypt functions.

Step5. The server publishes the elliptic curve parameters and the cryptographic functions described in step4.

B. User registration phase:

The user contacts the network administrator to get the following authentication information's as it is mentioned in Fig 2:

Step1. The user submits an identity and a password to the base station in a secure channel

Step2. BS computes the authentication key

$AK_U = H(ID_U \oplus password \oplus X)$ and

$H_U = H(ID_U \oplus password)$

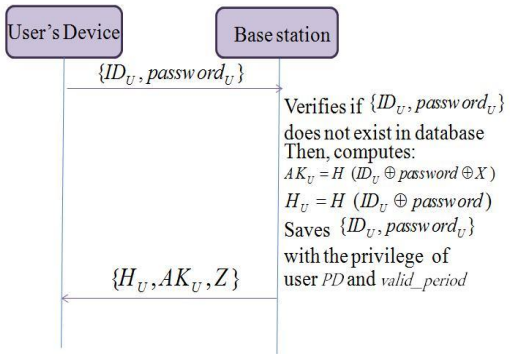

Fig2: user registration

Step3. BS delivers (**AKU,** H_U**,** Z) to the user in a secure channel

C. Mutual authentication with key agreement phase:

When the user sends a request to take information from the WSN, the authentication process schematized in Fig.3 starts:

Step1. GW $\longrightarrow$ **User:** M_1 (nonce)

GW generates a nonce and asks the user identity.

$H_U^* = HU$. If so, the user's device operates the nonce in the calculation of MAC_Z (IDU || nonce) using the shared key Z then it randomly chooses the point

$R_U(x_U, y_U) \in E_p(a, b)$ where x_U, y_U are co-ordinates M

$_U = R_U + (AK_U \cdot nonce) \cdot P$ and $R'_U = x_U \cdot P$.

Then, it sends

M (ID , non ce , M , R ' , MAC
2 U U U

To the gateways node.

Soon as the GW receives the message M_2 it checks if the nonce value exists or not in its temporary memory, if so it computes MAC_Z (ID_U & nonce) else it terminates the current session. After that, the GW verifies if the calculated MAC equals to the one received, if so the user with identity ID_U seems legitimate and the message is fresh then GW will query the BS to take supplementary information about the user U.GW forwards the identities ID_{GW} , ID_U to the BS and the Sequence number protected with he BS checks the sequence number, if it is bigger than the sequence number saved in its Database, it checks the MAC, if it is a valid MAC so the message is fresh and BS moves to the verification of the status of the customer in the Database.

$MAC_{X\,GW}(ID_{GW}, ID_U, seq\_num)$

Step3. GW $\longrightarrow$ **BS:**

$M_3 = (ID_U, seq\_num, MAC_{X\,GW}(ID_{GW}, ID_U, seq\_num))$

Upon receiving

$M_3 = (ID_U, seq\_num, MAC_{X\,GW}(ID_{GW}, ID_U, seq\_num))$

If the identity exists, BS checks the period of validity, if the identity does not exist or the period is over then the BS sends a message Reject_authentication to the gateways, if not the BS calculates to GW.

$AK_U = H(ID_U \oplus password \oplus X)$ and

$\beta = Encrypt_{Y\,GW}\{ID_u \| PD \| AK_u \| (seq\_num \oplus X_{GW})\}$

and sends the message $M4 = (\beta)$ soon as the GW receives M 4it decrypts β using its private key X GW, if the identity IDu is found in its temporary memory the GW calculates seq _ num ⊕ X GW and compares its value with that received, if they are equal so the gateways is sure that the ensure the legitimacy of the user

Step5. GW $\longrightarrow$ **U:** $M_5 = \{M_{GW}, M_k\}$

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

After receiving $M_5 = \{M_{GW}, M_k\}$, the user U computes $R_{GW}^* = M_{GW} - (AK_U \cdot nonce) \cdot P$ To derive R_{GW}^* (x_{GW}^*, y_{GW}^*). Then, U computes the equations $K^* = H(x_U, x_{GW}^*, nonce)$ and $M_k^* = (K^* + x_{GW}^*) \cdot P$ to check if $M_k^* = M_k$. If so, U can confirm that the GW is valid and the session key K^* is equal to k. Otherwise, the protocol is terminated.

V. SECURITY ANALYSIS:

In this section, we show how our proposed scheme can mitigate possible attacks.

❖ **Mutual authentication**

Mutual authentication means that both entities in a communication link authenticate each other. In our proposed scheme mutual authentication is assured between GW and BS, first the BS must be sure that the information or a request is going from a legitimate GW for that we use

MAC X GW (ID GW , IDU , seq _ num) which can be calculated only by the GW or the BS because they exclusively know the private key X GW . Second, the BS is authenticated

When both by the GW using the expression (seq _ num ⊕ X GW) in the encrypted message β . the validity of MAC X GW (ID GW , IDU , seq _ num) and (seq _ num ⊕ X GW) are confirmed by BS and GW

Respectively, the mutual authentication between them is achieved.

In this same context, both the gateway and the user must authenticate each other before generating the common session key. We can see that only the valid user and gateway can solve the other party's random points R_U and R_{GW} in the proposed scheme.

That is, both the user and the GW can authenticate the other party's validity. Thus, our scheme supports mutual authentication and it provides the reliability for the user and the GW both.

❖ **Key freshness**

Our scheme not only accomplishes the mutual authentication but also provides a session key between the user and the server that is necessary for the subsequent communications. Key freshness means that the key used in each session is different from the ones used in precedent sessions. Since each party picks his random point secretly when computing the session key in our protocol, it can be easily seen that the freshness of the used session keys in our scheme is guaranteed.

❖ **Preventing the replay attack**

Replay attack means that a legal peer's transmission messages is intercepted and replayed by an adversary to replay them later. However, the fresh **nonce** and **seq_num** chosen at each session are used to avoid such replay attacks in our scheme.

❖ **Preventing the insider attack**

Insider attack means that a legal client D can impersonate another legal client C to gain the service of the gateways. Assume that D wants to impersonate C to login to GW. However, without the knowledge AK_C, D cannot construct a valid message. Therefore, our scheme can withstand the insider attack.

VI. PERFORMANCE EVALUATION

In this section, we examine the performance of our proposed scheme. We present all cryptographic operations used in our protocol and we specify, for each member, the number of required operations during the authentication process in Table I.

TABLE I. PERFORMANCE IN THE LOGIN-AND AUTHENTICATION PHASE

Computational type	Number of use at		
	User	GW	BS
Random number generation	1	2	0
Hash operation	2	1	1
XOR function	1	1	2
Mac function	1	1	0
Point multiplication	4	4	0
Point subtraction	1	1	0
Encrypt operation	0	0	1
Decrypt operation	0	1	0

TABLE II. COMPUTATIONAL OVERHEAD FOR CRYPTOGRAPHIC OPERATION

Computational type	Execution time
Random number generation	400[µs]
Hash operation (SHA1)	14806 [µS]
MAC function (HMAC)	23[ms]
Point multiplication	2.5 [s]
Point substruction	193079[µs]
Encrypt operation (ECIES)	6.01[s]
Decrypt operation (ECIES)	3.9[s]

VII. CONCLUSION

In this paper we proposed a user authentication scheme based on the ABCRNG. The security of the scheme is based on a password memorized by the user and a secret key saved in user's device. We demonstrated the feasibility of ABCRNG in the context of WSNs.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

REFERENCES

[1] r authentication scheme for wireless sensor networks," In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06), vol. 1, Jun. 2006, pp. 244-251. Omar Cheikhrouhou, Anis Koubâa, Manel Boujelben and Mohamed Abid, "A Lightweight User Authentication Scheme for Wireless Sensor Networks", The ACS/IEEE Workshop : Future Trends on Ad- hoc and Sensor Networks (FT-ASN 2010), Hammamet, Tunisia, May 16-19, 2010.

[2] Sheetal Kalra and Sandeep K. Sood. "Elliptic curve cryptography: survey and its security applications". In Proceedings of the International Conference on Advances in Computing and Artificial Intelligence (ACAI '11). ACM, New York, NY, USA, 102-106. 2011.

[3] Haodong Wang, Bo Sheng, Chiu C. Tan, and Qun Li. "Public-key based access control in sensornet". Wirel. Netw. 17, 5 (July 2011).

[4] Sunil Gupta, Harsh Kumar Verma and AL Sangal "Authentication Protocol for Wireless Sensor Networks", World Academy of Science, Engineering and Technology 66 2010

[5] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, Sheueling Chang Shantz "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks" . In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PERCOM '05). IEEE Computer Society, Washington, DC, USA, 324-328. DOI=10.1109/PERCOM.2005.18

[6] Z. Benenson, F. Gartner, and D. Kesdogan, "User Authentication in Sensor Networks" (Extended Abstract), Lecture Notes in Informatics Proceedings of Informatik 2004, Workshop on Sensor Networks, Ulm, Germany, September 2004

[7] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing Robust User Authentication in Sensor Networks", in the Workshop on Real-World Wireless Sensor Networks, Sweden, June 2005.

[8] S. Banerjee and D. Mukhopadhyay. "Symmetric Key Based Authentication Querying in Wireless Sensor Networks", in Proceedings of the First International Conference on Integrated Internet Ad Hoc and Sensor Networks, Nice, France, May 30-31, 2006.

[9] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences", in Advances in Cryptology CRYPTO 92, LNCS 740, pp. 471486, 1993.

[10] Canming Jiang, Bao Li and Haixia Xu "An Efficient Scheme for User Authentication in Wireless Sensor Networks" 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 2007

[11] Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks", GLOBECOM 2007

[12] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic use.

[13] Huei-Ru Tseng, Rong-Hong Jan and Wuu Yang "A robust user authentication scheme with self-certificates for wireless sensor networks" Security and Communication Networks Security Comm. Networks (2010) Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/sec.212

[14] Rong FAN†, Dao-jing HE†‡, Xue-zeng PAN, Ling-di PING "Anefficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks" Journal of Zhejiang University- SCIENCE C (Computers & Electronics) ISSN 1869-1951 (Print); ISSN 1869-196X (Online) Received Oct. 27, 2010; Revision accepted Feb. 23, 2011; Crosschecked May 30, 2011

[15] Li F, Xin X, Hu Y. "Identity-based broadcast signcryption". Computer Standard and Interfaces 2008; 30:89–94

[16] Manel Boujelben, Omar Cheikhrouhou, Habib Youssef, Mohamed Abid. "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks", Third International Conference on Sensor Technologies and Applications, Greece, 18-23 June 2009.

[17] An Liu, Peng Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks" in Proceedings