2012 International Conference on Intelligent Information and Networks (ICIIN 2012)
IPCSIT vol. 23 (2012) © (2012) IACSIT Press, Singapore

Mutual Message Authentication Protocol in Wireless Sensor Networks

Yi-Hao Hong[+], Ya-Hui Zeng,Yu-Jung Huang

Department of Electronic Engineering, I-Shou University, Kaohsiung, Taiwan.

Abstract. Wireless sensor networks (WSNs) are through the distribution of sensor nodes in different locations to monitor environmental conditions. The collected data from sensor nodes were sent back to the base station for further analysis and processing. The protection of data confidentiality is the most critical requirements for the ubiquitous use of WSNs in various environments. This requires a secure and lightweight user authentication and access control. Symmetric key - based access control is not suitable for WSNs due to dynamic network topology, mobility, and stringent resource constraints. In this paper, we propose a secure, lightweight mutual authentication scheme, based on XOR operation generating a cover-coded pad function to protect the data. It can authenticate to an accessed node (a gateway node or sensor node) and vice versa. This is to ensure that data transmission is not exposed to an unauthorized person. On the other hand, it ensures that data sent to gateway/sensor did not originate from a malicious node. Simulation and hardware implementation results are presented to show advantages of the proposed scheme.

Keywords: Wireless Sensor Network, authentication protocol, security.

1. Introduction

Wireless sensor network (WSN, Wireless Sensor Network) is a kind of autonomous network with sensor nodes. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, humidity, sound, vibration, pressure, motion or pollutants [1].Sensors gather information about the physical world, e.g., the environment or physical systems, and transmit the collected data to controllers/actuators through single-hop or multi-hop communications. From the received information, the controllers/actuators perform actions to change the behavior of the environment or physical systems.

In WSN, It offers a limited amount of data reusability as local results from each participating node are passed to the base-station for further processing. However, wireless sensor networks are highly vulnerable to the failure of base stations. An adversary can render a wireless sensor network useless by launching remote, software based attacks or physical attacks on the base stations. This is because the WSN itself transmit messages through the wireless communication media. The attacker can access to make anonymous connections and the message is vulnerable to eavesdropping, interception and tampering. In WSN, the message exchange is through wireless access, if the information is not transmitted through the protection process, data messages will easily be stolen or received the fault message.

It is very important to protect the confidentiality of information and privacy for WSN network. In addition to those traditional security issues, many general-purpose sensor network techniques assumed that all nodes are cooperative and trustworthy. Therefore, mutual entity authentication plays an important role in securing wireless sensor networks. To enhance the security and privacy, a proposed mask function is used to establish mutual authentication protocol for WSN application. In this paper, we present a computationally efficient authentication framework, based on simple XOR operations, which makes it suitable for resource-restrained wireless sensor networks.

[+] Corresponding author.
E-mail address: sky0032@hotmail.com.

2. Related work

To distinguish legitimate users from intruders, authentication techniques are frequently used to verify the identity of the participants in a communication system. In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data transmitted was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then the behavior of the network could not be predicted and output as expected. There are several entity authentication schemes in wireless sensor networks have been proposed. Sastry and Wagner provided an access restriction on security in that the access control list (ACL) is applied to verify the client's authentication and arrange the nearest sensor node cooperating with the client. Watro et. al. [2] proposed an authentication protocol by applying intricate mathematical methods.

Benenson et al. proposed n-authentication protocol, in which the whole authentication succeeds if the user can successfully authenticate with any subset of sensors out of a set of nsensors. Based on elliptic curve cryptography, Benenson, Gedicke, and Raivio introduced an entity authentication scheme of WSNs. Jiang and Xu [3] proposed a distributed entity authentication scheme in wireless sensor networks. It is established on the self-certified keys cryptosystem, which is modified to use elliptic curve cryptography to set up pair-wise keys for use in the entity authentication scheme. Tripathy and Nandi [4] used cellular automata based components to achieve entity authentication. Cagalj et al. [5] propose integrity codes (Icodes) to support message integrity checks. Using only the properties of the wireless channel and radio transmissions, I-codes enable a broadcast message authentication and the concept of "authentication through presence". Wong et al. [6] proposed a dynamic strong-password-based entity authentication scheme for WSNs; which consists of three phases: Registration, Login, and Authentication. Later, Tseng et al. [7] pointed out several weaknesses in Wong et al.'s scheme, and proposed an improved scheme to overcome the weaknesses and allow legitimate users to change their password freely. Thus, it consists of four phases: Registration, Login, Authentication, and Password changing. Ko [8] showed that Tseng et al.'s scheme still comes with several drawbacks that might cause authentication mechanism insecure; thus proposed a novel scheme, which not only inherits all the advantages of Tseng et al.'s scheme but also achieves mutual authentication and enhances its security strength. Das [9] proposed a two-factor user authentication for WSNs, claiming that the mechanism could avoid not only replay and stolen-verifier attacks but also the guessing and masquerade attacks. Vaidya et. al. [10] proposed an improved robust user authentication scheme for wireless sensor networks. However, most of the above-mentioned schemes have not given any results implemented in hardware.

3. Cover-coded pad operation

In order to achieve the low computational cost, a cover-coded pad function is used to protect the data for wireless transmission.

Let us represent the 32-bit password and 32-bit message in binary (Base 2) as

$$\text{Apwd} = a_0 a_1 a_2 a_3 \ldots a_{31} \tag{1}$$

$$\text{Messg} = m_0 m_1 m_2 m_3 \ldots m_{31} \tag{2}$$

The 16-bit random numbers R_{Tx} and R_{Kx} in hexadecimal (Base 16) are

$$R_{Tx} = d_{t1} d_{t2} d_{t3} d_{t4} \tag{3}$$

$$R_{Kx} = d_{k1} d_{k2} d_{k3} d_{k4} \tag{4}$$

Each digit of R_{Tx} and R_{Kx} is used to indicate a bit location in Apwd, and these bits are concatenated to form a 16-bit output in hexadecimal (Base 16) representations as

$$\begin{aligned} &\text{Apwd} - \text{PadGen}\left(R_{Tx}, R_{Kx}\right) = \\ &a_{d_{t1}} a_{d_{t2}} a_{d_{t3}} a_{d_{t4}} \left\| a_{d_{t1}+16} a_{d_{t2}+16} a_{d_{t3}+16} a_{d_{t4}+16} \right\| \\ &a_{d_{k1}} a_{d_{k2}} a_{d_{k3}} a_{d_{k4}} \left\| a_{d_{k1}+16} a_{d_{k2}+16} a_{d_{k3}+16} a_{d_{k4}+16} \right. \\ &= d_{v1} d_{v2} d_{v3} d_{v4} \end{aligned} \tag{5}$$

where $d_{v1}d_{v2}d_{v3}d_{v4}$ is the decimal (Base 10) notation. The PadGen is again performed over Kpwd using the above generated $d_{v1}d_{v2}d_{v3}d_{v4}$ to indicate a bit location in Kpwd, and these bits are concatenated to form a 16-bit PAD. The resulting PAD would then be expressed as

$$\begin{aligned}
&\mathrm{PAD} = \mathrm{Messg} - \mathrm{PadGen}(\mathrm{Apwd} - \mathrm{PadGen}(\mathrm{R_{Tx}},\mathrm{R_{Kx}}),\mathrm{R_{Tx}}) \\
&= \mathrm{Messg} - \mathrm{PadGen}(d_{v1}d_{v2}d_{v3}d_{v4}, R_{Tx}) \\
&= m_{d_{v1}} m_{d_{v2}} m_{d_{v3}} m_{d_{v4}} \left\| m_{d_{v1}+16} m_{d_{v2}+16} m_{d_{v3}+16} m_{d_{v4}+16} \right\| \qquad (6) \\
&\quad m_{t1}m_{t2}m_{t3}m_{t4} \left\| m_{t1+16} m_{t2+16} m_{t3+16} m_{t4+16} \right. \\
&= h_{p1}h_{p2}h_{p3}h_{p4}
\end{aligned}$$

where $h_{p1}h_{p2}h_{p3}h_{p4}$ is the hexadecimal (Base 16) notation.

This proposed mutual authentication protocol WSN divided into three phases, the Registration phase, Login phase, and the Authentication phase. In our proposed scheme, it is assumed that the sensor node has the capability to verify two passwords access password (APwd) and message (Messg). A gateway that presents the right APwd, is allowed to carry out mandatory commands such as Read, Write, and Lock on the node. If a gateway sends the right Messg, the node enters into the secured state. Gateway can generate 16-bit random or pseudo-random numbers RTx. While powered, Gateway can temporarily store at least two pseudo-random numbers RTx. Gateway and Sensor Node implement an Access command; which causes the node to transition from the open to the secured state. Gateway and Sensor Node can communicate indefinitely in the secured state. Just prior to issuing each Access command the Gateway first issues a command ReqR requesting a random number. RTx is used has XOR pad to obscure APwd, this is known as Cover-Coding APwd (CCPwd). Each XOR operation shall be performed first on APwd's 16-Most Significant Bits (MSB) denoted as $\mathrm{APwd_M}$, followed by 16-Least Significant Bits (LSB) denoted as $\mathrm{APwd_L}$. In a similar way, the message delivery can be protected using XOR operation with the cover-coded pad. Each XOR operation shall be performed first on Mesg's 16-Most Significant Bits (MSB) denoted as $\mathrm{Messg_M}$, followed by 16-Least Significant Bits (LSB) denoted as $\mathrm{Mesg_L}$.

$$\mathrm{CCPwd_{M1}} = \mathrm{APwd_M} \oplus \mathrm{PAD_1} \qquad (7)$$

$$\mathrm{CCPwd_{L1}} = \mathrm{APwd_L} \oplus \mathrm{PAD_2} \qquad (8)$$

$$\mathrm{CCMsg_{M1}} = \mathrm{Mesg_M} \oplus \mathrm{PAD_3} \qquad (9)$$

$$\mathrm{CCMsg_{L1}} = \mathrm{Mesg_L} \oplus \mathrm{PAD_4} \qquad (10)$$

4. Proposed authentication schemes

An improved version of the mutual authentication process is demonstrated as shown in Fig. 1. The proposed two-way authentication protocol is divided into three phases: registration, login and authentication. **Table 1** lists the symbols for the operation of the proposed two-way authentication protocol.

Table I. Customized authentication WSN symbol definition table

Symbol	Description	*M*	Cover Coding Message	*K*	Cover Coding Key
HASFn()	Coding Function	*MACC*	Message Authentication Code	*x*	Client Key
UrKey	Client Password	*IDGK, IDSK*	Authentication Key	$\oplus$	XOR
RN	Random Number (Publicity)	$\|$	Connection between bits	*TS*	Timestamp
RM	Random Number (Privacy)	ΔT	Reasonable Time	*Msseg*	Message
PW	Access Password	*ID*	Identity Verification		

The flow procedures for the registration phase are shown in Fig. 1. Firstly, user sends a UserID and Req to the sensor gateway. After receiving the message, the gateway will generate and store ($\mathrm{Rt_1}$, $\mathrm{Rt_2}$, $\mathrm{Rm_1}$, $\mathrm{Rm_2}$) and ($\mathrm{Rt_3}$, $\mathrm{Rt_4}$, $\mathrm{Rm_3}$, $\mathrm{Rm_4}$). Then, Gateway transmitted ($\mathrm{Rt_1}$, $\mathrm{Rt_2}$, $\mathrm{Rm_1}$, $\mathrm{Rm_2}$) to the user and transmitted ($\mathrm{Rt_3}$, $\mathrm{Rt_4}$, $\mathrm{Rm_3}$, $\mathrm{Rm_4}$) to sensor nodes. The user receives ($\mathrm{Rt_1}$, $\mathrm{Rt_2}$, $\mathrm{Rm_1}$, $\mathrm{Rm_2}$) from the gateway and applies PadGen ($\mathrm{Rt_1}$, $\mathrm{Rm_1}$), PadGen ($\mathrm{Rt_2}$, $\mathrm{Rm_2}$) algorithm to generate ($\mathrm{Pad_1}$, $\mathrm{Pad_2}$), then performs $\mathrm{APwd_M} \oplus \mathrm{Pad_1}$ and $\mathrm{APwd_L} \oplus \mathrm{Pad_2}$ operation to get ($\mathrm{CCPwd_{M1}}$, $\mathrm{CCPwd_{L1}}$). User then sends message ($\mathrm{CCPwd_{M1}}$, $\mathrm{CCPwd_{L1}}$) to gateway. Gateway applies PadGen ($\mathrm{Rt_1}$, $\mathrm{Rm_1}$), PadGen ($\mathrm{Rt_2}$, $\mathrm{Rm_2}$) algorithm to generate ($\mathrm{Pad_3}$, $\mathrm{Pad_4}$), and solved ($\mathrm{APwd_M}$, $\mathrm{APwd_L}$) using ($\mathrm{CCPwd_{M1}}$, $\mathrm{CCPwd_{L1}}$) received from users.

In addition, Gateway also utilizes PadGen (Rt_3, Rm_3), PadGen (Rt_4, Rm_4) algorithm to generate (Pad_5, Pad_6), then performs $APwd_M \oplus Pad_5$ and $APwd_L \oplus Pad_6$ to get ($CCPwd_{M2}$, $CCPwd_{L2}$) ($CCPwd_{M2}$, $CCPwd_{L2}$) along with the UserID will be sent to the sensor nodes from the Gateway. Sensor node received ($CCPwd_{M2}$, $CCPwd_{L2}$) from the gateway, applies PadGen (Rt_3, Rm_3), PadGen (Rt_4, Rm_4) algorithm to solve ($APwd_M$, $APwd_L$). Finally, based on whether ($APwd_M$, $APwd_L$) is correct or not to decide whether the registration process is completed or not.

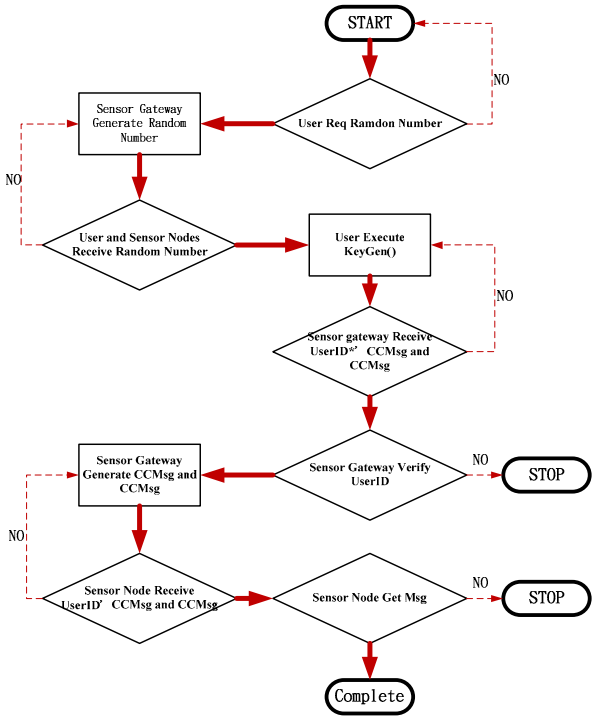

Fig. 1 Registration Phase

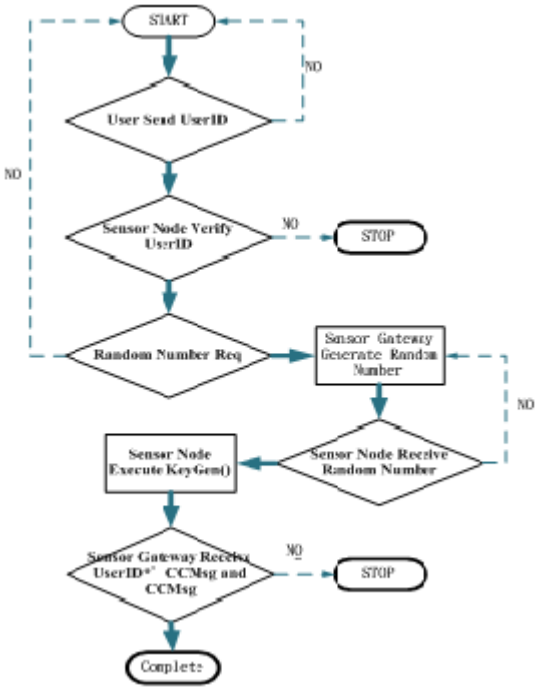

Fig. 2 Login Phase

The login phase contains seven steps as shown in Fig. 2. The registration phase starts when user send a UserID * to sensor nodes. Sensor node will then verify the UserID * and sends the request to gateway. After receving the request from senor node, Gateway generates and stores (Rt_5, Rt_6, Rm_5, Rm_6). In the meantime, Gateway transmits (Rt_5, Rt_6, Rm_5, Rm_6) to sensor nodes. Sensor node applies PadGen (Rt_5, Rm_5), PadGen (Rt_6, Rm_6) algorithm to generate (Pad_9, Pad_{10}), then perform $APwd_M \oplus Pad_9$ and $APwd_L \oplus Pad_{10}$ operation to get ($CCPwd_{M3}$, $CCPwd_{L3}$) and ($CCPwd_{M3}$, $CCPwd_{L3}$). Finally, sensor node send back UserID* along with ($CCPwd_{M3}$, $CCPwd_{L3}$) to complete the login process.

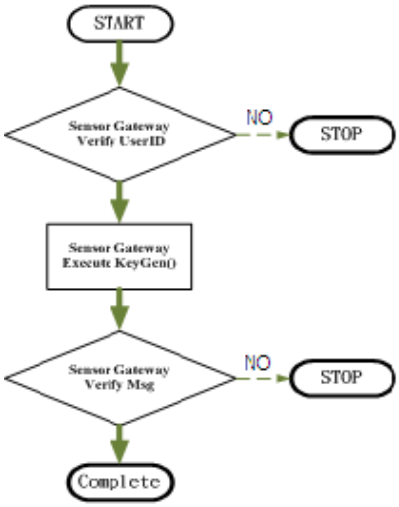

Fig. 3 Authentication Phase

The authentication phase is shown in Fig. 3. The detail description about the authentication phase is as follows. Gateway firstly verify whether the UserID* is equal to UserID. If UserID * is correct, then gateway performs $CCPwd_{M3} \oplus PAD_{10}$, $CCPwd_{L3} \oplus PAD_{11}$ to get ($Apwd_M$*, $Apwd_L$*). If Pwd* = Pwd, gateway sends message Msg (ACC_LOGIN) to the sensor node and users to complete the authentication phase.

5. Hardware implementation

According to the mutual authentication described in the previous section, a proposed hardware architecture is shown in Fig. 4:

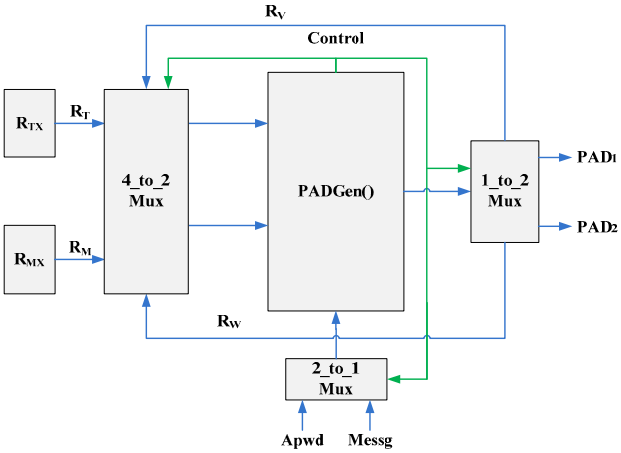

Fig. 4 Mutual Authentication Hardware Architecture

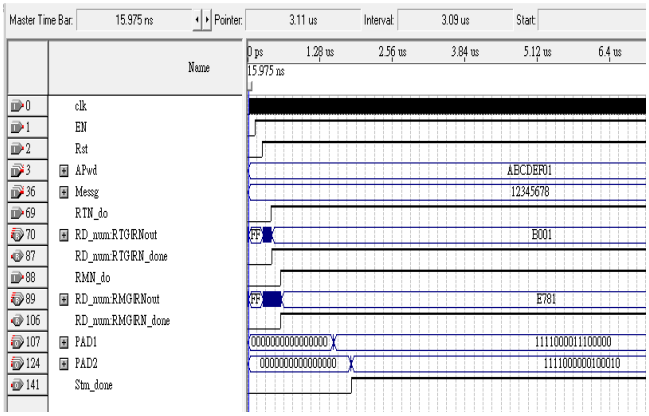

Fig. 5 Simulation Results of PAD1 and PAD2

After the initial input of R_{Tx} and R_{Mx}, a multiplexer was utilized to allow for the selection of Apwd or Msseg for PadGen() XOR operation. The detail functions performed by Fig. 4 are described as follows. R_T, R_M, and Apwd are selected as PadGen () input, the calculation results of PadGen () are APwd-PadGen (R_T, R_M) = dv1dv2dv3dv4 = R_V . The operation of $R_T \oplus R_V$ and $R_T \oplus R_M$ are performed and their results along with Apwd are used as input for PadGen (). The calculation results of PadGen () are APwd-PADGen ($R_T \oplus R_V$, $R_T \oplus R_M$) = dw1dw2dw3dw4 = R_W The PAD_1 can then be obtained from the output of PadGen () using R_T, R_M, and Messg as input for PadGen (). Messg-PadGen (RV, RW) = dx1dx2dx3dx4 = PAD_1. The operation of $R_T \oplus R_V$ and $R_T \oplus R_M$ are performed and their results along with KPwd are used as input for PadGen ().the PAD_2.can then be obtained from the output of PadGen (). Messg-PADGen(RM⊕RV,RV⊕RW)=dy1dy2d y3d y4 = PAD.For RT =B001, RM = E781, APwd=12345678, and Messg=ABCDEF01, the simulation results of the PAD1=1111 _0000_1110_0000 and PAD2= 1111_0000_0010_0010. are shown in Fig. 5.

The verified verilog code was downloaded on an Altera Cyclone II FPGA in the Altera DE2 Board for hardware verification. TheLED shows PAD1=F0E0 (hex) and PAD2=F022 (hex) as depicted in Figs. 6, respectively.

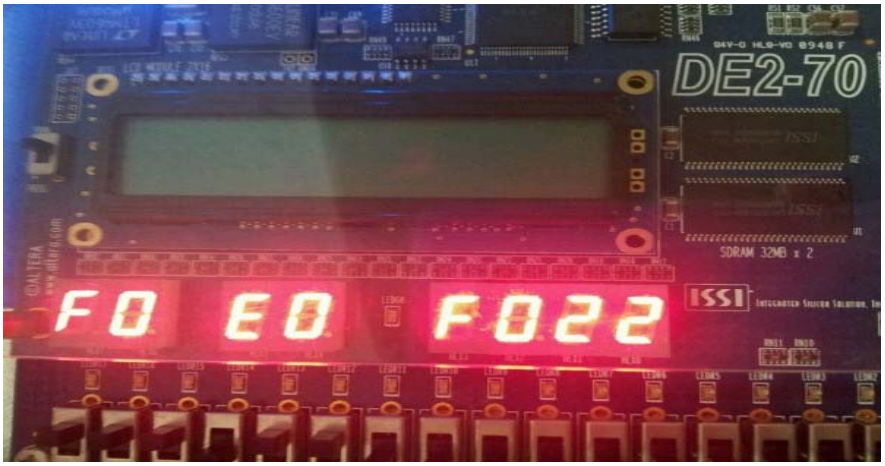

Fig. 6 PAD1 and PAD2 on the Altera DE2-70

6. Conclusion

One of the most critical security concerns before deploying a WSN in real world applications is privacy issues. To achieve this, authentication and access control must be enforced to ensure secure data transmission originated from legitimate sensors. This paper introduces a light way cryptography method called cover-coded pad generation function (PadGen). PadGen provides cover-coded password and message for mutual authentication (a user can authenticate to a Gateway and through Gateway to the sensor nodes and vice versa). PadGen function provides light weight computional cost and requires lesser memory, which makes it practically feasible to be implemented on sensor platforms. The corresponding hardware architecture is also simulated using Verilog hardware description language to validate the functionality of the proposed architecture. In addition, the FPGA implementation on Altera DE2 demo board is presented. The feasibility of the present mutual authentication protocol can be used in WSN systems is successfully demonstrated.

7. Acknowledgement

This work was supported in part by the National Science Council, Taiwan, under Grants NSC98-2221-E-214-047.

8. References

[1]Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine. 2002;40(8):102–114.

[2]R. Watro, D. Kong, Sue-fen Cuti, C. Gardiner, C. Lynn and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," *Proc. ACM WorkshopSecurity Ad Hoc Sensor Netw.*, 2004, pp. 59-64.

[3]Jiang C, Li B, Xu H. An Efficient Scheme for User Authentication in Wireless Sensor Networks. In: 21st International Conference on Advanced Information Networking and Applications Workshops; 2007. p. 438–442.

[4]Tripathy S, Nandi S. Defense against outside attacks in wireless sensor networks. Computer Communications. 2008;31(4):818–826.

[5]M. ˇCagalj, S. ˇCapkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava, and J.-P. Hubaux, "Integrity (I) Codes: Message Integrity Protection and Authentication Over Insecure Channels," in *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)*, May 2006, pp. 280–294.

[6]Wong KHM, Zheng Y, Cao J,Wang S. A Dynamic User Authentication Scheme for Wireless Sensor Networks. In: IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06); 2006. p. 244–251.

[7]Tseng HR, Jan RH, Yang W. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks. In: IEEE Global Telecommunications Conference (GLOBECOM '07); 2007. p. 986–990.

[8]Ko LC. A novel dynamic user authentication scheme for wireless sensor networks. *Proceedings of the IEEE International Conference on (IEEE ISWCS 2008)*, Reykjavik, Iceland, October 2008; 608–612.

[9]M.L. Das, "Two-Factor User Authentication in Wireless Sensor Networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, 2009, pp. 1086-1090.

[10] B. Vaidya, M. Chen, and J. Rodrigues, "Improved Robust User Authentication Scheme for Wireless Sensor Networks," *5th IEEE Proc. Wireless Commun. Sensor Networks,* 2009, pp. 1-6.