CSIT (March 2014) 2(1):35–41
DOI 10.1007/s40012-014-0042-8

Efficient security mechanism to counter the malicious attack in wireless sensor networks

Sunil Gupta · Harsh K. Verma · A. L. Sangal

Received: 24 January 2014 / Accepted: 4 June 2014 / Published online: 8 July 2014

Abstract Security in wireless sensor network (WSN) is a critical issue when it comes to malicious attack or power loss. Recently, several security mechanisms have been proposed. In this paper, an efficient security mechanism is proposed to provide better authentication mechanism to counter the malicious attacks in WSN. The proposed protocol is well designed for sensor node, which has limited resources with a better authentication by using a one way hash function and smart card. In this paper, we pointed out several pitfalls in previous schemes and proposed an improvement that will result in better resource utilization and better security. The security analysis shows that proposed protocol defend better and provide cost effective mechanism to defend against malicious attack.

Keywords Authentication · Wireless sensor networks · Wireless security · Hash function · Smart card · Malicious attack

1 Introduction

Security allows wireless sensor network (WSN) to be used with assurance. Without security, the use of WSN in any application area would cause undesirable consequences. WSN are rapidly gaining popularity due to low cost solutions to a variety of real world challenges. The basic idea of a sensor network is to disperse tiny sensing devices, which are capable of sensing some changes of parameters. WSN can communicate with other devices over a specific geographic area for some particular purpose like surveillance, environmental monitoring and target tracking etc. [1].

In case of WSN, the communication between the sensors is done using wireless transceivers. The major challenge of employing any efficient security scheme in WSN is created by the size of sensors which can affect memory and processing power [2]. To deal with the important security issues in WSN we talk about cryptography, steganography and other basics of network security alongwith their applications. We investigate various types of threats and attacks against WSN to save manufacturing cost. A sensor node is usually built as a small device, which has limited memory, a low-end processor, and is powered by a battery. So during the design of any security solution we need to take care of resource constraints like limited energy, limited memory, limited computing power, limited communication bandwidth and limited communication range.

The type of security mechanism that can be hosted on a sensor node platform is dependent on the capabilities and constraints of sensor node hardware. Some of the nodes in the network may weaken their power because of the irregular distribution of traffic load after several weeks or months of operation. Therefore, deployment of new node is needed in this case. Besides the natural loss of sensor nodes, a sensor network is also vulnerable to malicious attacks in unattended and hostile environments. Some of the sensor nodes may be destroyed by an opponent, so that the entire network may become useless and new sensor nodes can be deployed. On the other hand, an opponent can also position malicious nodes in the network. These malicious nodes may insert false reports [3]. Recently many schemes have been proposed to defend the sensor networks. The authentication procedure is needed to differentiate malicious ''new'' nodes, from legitimate new

S. Gupta (✉) · H. K. Verma · A. L. Sangal
Department Of Computer Science & Engineering,
Dr. B. R. Ambedkar National Institute of Technology,
Jalandhar, Punjab, India
e-mail: research.sunil@gmail.com

nodes. The authentication protocol mentioned in the paper will help the new node in establishing shared keys with its neighbors, so that it can perform secure communications with its neighbors.

2 Related works

Wong et al. [4] proposed a "Scalable Group Key Management Protocol" using key graphs. According to him, one might utilize keys of multiple granularities to reduce the re-keying overhead associated with membership management. Wong also investigates multiple approaches for constructing re-keying messages.

Sharifi et al. [6] presented that "SKEW" is a lightweight protocol for key management in WSN. It tries to manage keys with minimum communication, key transmission and storage usage. It is a base key management protocol that preserves network security before start up.

Edmond Holohan & Michael [7] have introduced AVCA, "Authentication uses Virtual Certificate Authorities", which is a PKI architecture. It is based on commonly used and well established PKI concepts and designed specifically for resource constrained devices on distributed ad-hoc networks. It provides a mechanism to overcome the difficulties in securing many distributed networks with non tamper-proof devices.

Jiang, Li, Xu [8] have proposed an efficient user authentication scheme based on the self-certified keys cryptosystem (SCK) to establish pairwise keys. The proposed scheme not only provide a variety of security features, but also efficient in terms of message exchanges and computational burdens.So, it can be easily implemented in the real WSN. Author scheme is based on the SCK cryptosystem to establish pairwise keys.

Tseng et al. [9] proposed an improved "Dynamic User Authentication Scheme" for WSN. Their scheme is divided into four phases, i.e., the registration phase, the login phase, the authentication phase and the password change phase. The registration phase is performed only once via a secure channel. The login phase is executed whenever a registered user wants to retrieve sensor readings from the nearest sensor login-node. The author sends the query to the sensor login-node by using mobile devices. The authentication phase is started whenever the gateway receives the user's login message forwarded from the sensor login-node. Upon receiving the message from the sensor login-node, the gateway checks the user's authenticity and replies the checking result to the sensor login-node. The password change phase is started whenever the users want to change their password via a secure channel.

Ko [10] proposed improved scheme by modifying Tseng [9] scheme.

Benenson et al. [11] proposed a protocol for WSN, where user can successfully authenticate with any subset of sensors out of a set of n sensors.

Arikumar, Thirumoorthy [12] proposed an "Improved User Authentication in Wireless Sensor Networks". The basic idea of the protocol is that a user will receive a personalized smart card from the GW-node at the time of the registration process and then with the help of user's password and smart card the user can login to the sensor/GW node and access data from the network.

Das [13] have proposed "Two-Factor User Authentication Protocol" for WSN which provides strong authentication an session key establishment to achieve efficiency.

Huang, Chang [14] proposed an "Enhancement Of Two Factor User Authentication In Wireless Sensor Network". Das's [13] proposed a two-factor user authentication scheme in wireless sensor networks.

Vaidya, Makrakis, Mouftah [15] proposed an "Improved Two-Factor User Authentication in Wireless Sensor Networks". This new scheme can overcome the pitfalls in Das's [13] and Algahathbar's [17] schemes as well as provide robustness and higher level of security.

He, Gao, Chang, Chen, bu [16] proposed an enhanced scheme based on Das Scheme [13], which keeps the merits of the original protocol and can withstand the security weaknesses described in the previous section.

Khan, Alghathbar [17] proposed "Cryptanalysis And Security Improvements of Two-Factor User Authentication In Wireless Sensor Networks". He shows that the Das-scheme [13] has some critical security pitfalls and cannot be recommended for real applications.

Yeh, Chen, Liu, Kim, Wei [18] have proposed "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography" and he review several proposed WSN user authentication protocols, with a detailed review of the Das protocol [13] and a cryptanalysis of Das's protocol that shows several security weaknesses.

Sarika, Nawaz [19] proposed a "User Authentication Framework for Wireless Sensor Networks" which ensures the access and supply of data taking place by the legitimate users only. A user must register with the gateway node in a secure manner to access the real time sensor data. Upon the successful user registration, the gateway node personalizes a smart card to every registered user.

3 The proposed authentication mechanism

To avoid the GW-node impersonation attack and the GW node bypassing attack. The crucial idea is that the GW-node distributes the different secret keys for each Ui and each Sn. We can intuitively see that Ui cannot impersonate

Table 1 Notation used in proposed scheme

Symbol	Description
U_i	User
IDi	Identity
Pwi	Password choosen
h (), h 1	Cryptographic hash Function
||	Concatenation
T	Time stamp
K	Symmetric key
N1, N2, N3	Nonce
Sn	S-node
GW-node	Gateway node
ΔT	Expected time interval

the GW node without its secret key. For the same reason, the adversary owning one Sn's secret key is difficult to bypass the GW-node to access other S-nodes without their corresponding secret keys. Hence, we require that the GW-node generates the parameters SIDn and the h(SIDn||K) and writes them in Sn before deploying the WSN, where h(SIDn||K) is treated as Sn's secret key. Following the historical tradition, the proposed scheme composed of four phases, that is, the registration phase, the password change phase, the login phase and the authentication phase. The notation used throughout paper is shown in Table 1.

3.1 Registration phase

In the first phase user, Ui wants to register with the WSN.

Step 1 User Ui wants to submit his identification IDi to the gateway node passed over the secure channel.

Step 2 The Gateway node verifies IDi after receiving the registration request from user Ui and generate Vi = h{(IDi||K)||h(Pwi)}. The gateway node generates the values with the function h () & h1 () and then Store them in the smart card.

Step 3 Pwi is Gateway node provides the smart card and password (Pwi) to the user through a secure channel. The initial password is provided by the Gateway node due to which this scheme is not secured from privileged-insider attack. This is recommended when user Ui receives the smart card and then immediately change the login password using the password change phase.

3.2 Login phase

When user Ui want to access data or wants to perform some query for WSN then login phase will start immediately.

Step 1 User Ui wants to perform a query, then he has to provide user IDi and Password Pwi; however first of all user Ui has to insert his smart card in the terminal. After inserting a smart card in the terminal user, Ui will provide IDi and Pwi. Now smart card will check the entered values with the previously stored values; if both the values with each other matches then smart card will generate a hello packet to Gateway node. If the values does not match with each other then the login request will be rejected.

Step 2 After getting a hello packet from the user Ui, Gateway node will generate N1 and send it to the smart card.

Step 3 After receiving N1 from Gateway node, smart card calculates Ai = h1(Vi_h(Pwi))||N1 and h(K||T). Where T is the current timestamp and K, is the secret key. After that smart card sends IDi, Ai, and h(K||T) to the Gateway node.

Step 4 After receiving Ai, IDi, h(K||T), Gateway node verifies the validity of time with ΔT = T2−T1. If it is found true, then it checks Ai? = h1(h(IDi||K) ||N1),using the secret key K. If either of IDi or Ai is invalid then Ui request login is rejected, and the session will be terminated. Otherwise, the Gateway node approves the Ui login request.

3.3 Authentication phase

After the login phase is done, the GW-node will generate N2 and sends a message {IDi, N2} to some nearest Sn over a public channel to respond to the query or the data which Ui is looking for.

Step 1 Upon receiving the message {IDi, N2}, the designated Sn generates N3 and computes Bi = h1(h(SIDn||K)||IDi||N2||N3) using the secret key.h(SIDn||K). Then, Sn sends the message {SIDn, Bi, N3} to the GW-node.

Step 2 Upon receiving the message {SIDn, Bi, N3}, the GW-node checks the validity of SIDn and Bi? = h1(h(SIDn||K)||IDi||N2||N3) using the secret key K. If any verification fails, the GW-node terminates the session. Otherwise, the GW-node computes the value Ci = h1(IDi||h(SIDn||K)||N3||N2) and is sent to the mutual authentication message {Ci} to Sn.

Step 3 Upon receiving the message {Ci}, Sn verifies whether Ci? = h1(IDi||h(SIDn||K)||N3||N2). If Ci is invalid, Sn terminates the session. Otherwise, Sn sends a successful signal to the GW-node.

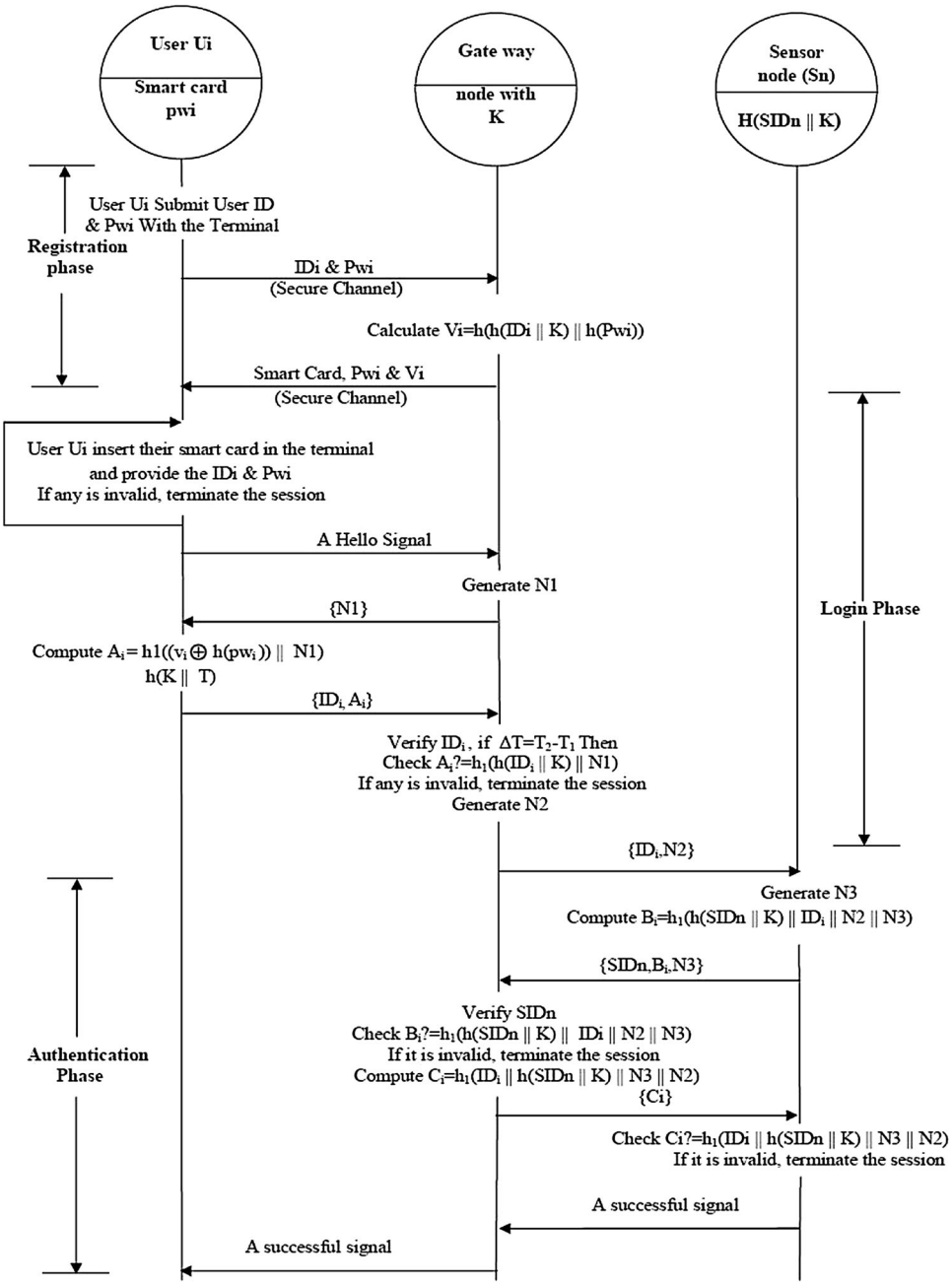

Fig. 1 The proposed authentication mechanism

Step 4 Upon receiving the successful signal, the GW node further sends a successful signal to Ui, and the session is successful. We simply depict the user authentication session as shown in Fig. 1.

3.4 Password change phase

This phase is invoked whenever Ui wants to alter his password pwi with a new one, say pw × i.

Step 1 Ui attaches his smart card to the smart card reader of a terminal, enters his IDi, pwi, and pw × i, and requests to alter the password.

Step 2 Ui's smart card validates the entered parameter IDi using the previously stored value. If IDi is correct, then Ui will be able to change the password. Otherwise, the password change phase is completed.

Step 3 Ui's smart card calculates V × i = Vi_h(pwi)_h(pw × i), and then change the old value Vi with the new value V × i.

Note Ui can freely change his password without any communication with the GW-node. Because the GW-node cannot touch any Ui's password information, this design prevents the possibility of the privileged-insider attack.

Table 2 Computational cost of different schemes

Phase	Wong [4]	Tseng et. al. [9]	Lee et. al. [3]	Das [13]	He [16]	Algahathour [17]	Huang [14]	Vaidya [15]	Arikuma [12]	Yeh [18]	Sun et al. [5]	Proposed protocol
Registration	$2T_H$ + $1C_{MH}$	$1T_H$ + $1C_{MH}$	$2T_H$ + $2T_{XOR}$ + $1C_{MH}$	$2T_H$ + $1T_{XOR}$ + $1C_{MH}$	$5T_H$ + $4T_{XOR}$ + $1C_{MH}$	$3T_H$ + $3T_{XOR}$ + $1C_{MH}$	$3T_H$ + $1T_{XOR}$ + $1C_{MH}$	$5T_H$ + $3T_{XOR}$ + $1C_{MH}$	$3T_H$ + $1T_{XOR}$ + $1C_{MH}$	$2T_H$ + $2T_{XOR}$ + $1C_{MH}$	$2T_H$ + $1T_{XOR}$ + $1C_{MH}$	$1T_H$ + $1T_{XOR}$ + $1C_{MH}$
Login	$2T_H$ + $2T_{XOR}$ + $1C_{MH}$	$2T_H$ + $2T_{XOR}$ + $1C_{MH}$	$3T_H$ + $3T_{XOR}$ + $1C_{MH}$	$3T_H$ + $1T_{XOR}$ + $1C_{MH}$	$4T_H$ + $4T_{XOR}$ + $1C_{MH}$	$6T_H$ + $2T_{XOR}$ + $1C_{MH}$	$3T_H$ + $1T_{XOR}$ + $1C_{MH}$	$6T_H$ + $2T_{XOR}$ + $1C_{MH}$	$4T_H$ + $2T_{XOR}$ + $1C_{MH}$	$3T_H$ + $3T_{XOR}$ + $1C_{MH}$	$2T_H$ + $1T_{XOR}$	$3T_H$ + $1T_{XOR}$ + $1C_{MH}$
Authentication	$1T_H$ + $1T_{XOR}$ + $1C_{MH}$	$2T_H$ + $2T_{XOR}$ + $1C_{MH}$	$11T_H$ + $13T_{XOR}$ + $1C_{MH}$	$5T_H$ + $2T_{XOR}$ + $1C_{MH}$	$6T_H$ + $2T_{XOR}$	$7T_H$ + $4T_{XOR}$ + $1C_{MH}$	$5T_H$ + $2T_{XOR}$ + $1C_{MH}$	$7T_H$ + $4T_{XOR}$	$7T_H$	$6T_H$	$5T_H$+	$4T_H$ + $1C_{MH}$
Password change	–	–	–	–	$2T_H$ + $2T_{XOR}$	$2T_H$ + $2T_{XOR}$	$2T_H$ + $1T_{XOR}$ + $1C_{MH}$	$6T_H$ + $6T_{XOR}$	–	–	$2T_H$ + $1T_{XOR}$	$2T_H$ + $1T_{XOR}$ + $1C_{MH}$
Total cost	$5T_H$ + $3T_{XOR}$ + $3C_{MH}$	$5T_H$ + $4T_{XOR}$ + $3C_{MH}$	$16T_H$ + $18T_{XOR}$ + $3C_{MH}$	$10T_H$ + $4T_{XOR}$ + $3C_{MH}$	$17T_H$ + $12T_{XOR}$ + $4C_{MH}$	$18T_H$ + $11T_{XOR}$ + $4C_{MH}$	$13T_H$ + $5T_{XOR}$ + $4C_{MH}$	$24T_H$ + $15T_{XOR}$ + $4C_{MH}$	$14T_H$ + $3T_{XOR}$ + $3C_{MH}$	$11T_H$ + $5T_{XOR}$ + $3C_{MH}$	$11T_H$ + $3T_{XOR}$ + $4C_{MH}$	$10T_H$ + $3T_{XOR}$ + $4C_{MH}$

4 Security analysis

This security mechanism can effectively defend node importation attack and by passing.The comparative study chart is as shown in Table 2 shows the proposed framework has less computational cost and overhead as compared to the respective other protocol.

4.1 Computational cost

In Table 2, one might observe the computational cost of user registration, login phase, authentication phase & password change phase. we tabulated the computational cost of user registration, login phase, authentication phase and password change phase. Here, one might take hash value with bitwise operation. One can observe that the proposed scheme provides better security and less computational cost as compared to the previous schemes.

4.2 Communication cost

In each session of registration, login, authentication and password change, one requires less exchange of message with better computational speed, efficiency and implementation of password change with the use of timestamp.

Considering the above parameters of computational cost, its communication cost and above comparison, we infer that the proposed scheme is much more efficient as compared to other schemes.

Our analysis shows the effectiveness as against malicious attack. The comparative study chart is as shown in Table 1. It shows the proposed framework has less computational cost and overhead as compared to the respective other protocol. Figures 2, 3, 4, 5, 6 and 7 shows the comparative analysis on the base of cost and overhead of one way hash function and bit wise XOR function.

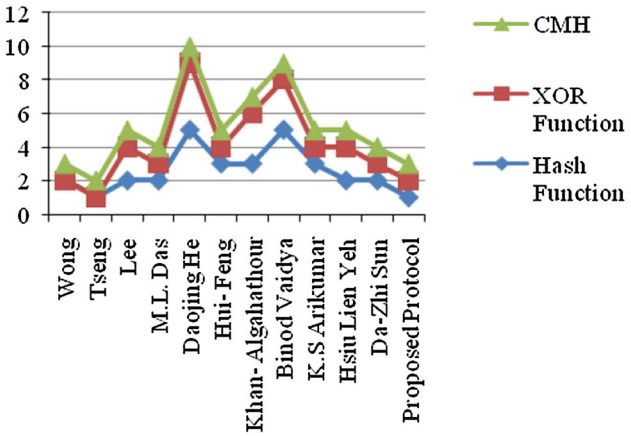

Fig. 2 Registration phase for protocols

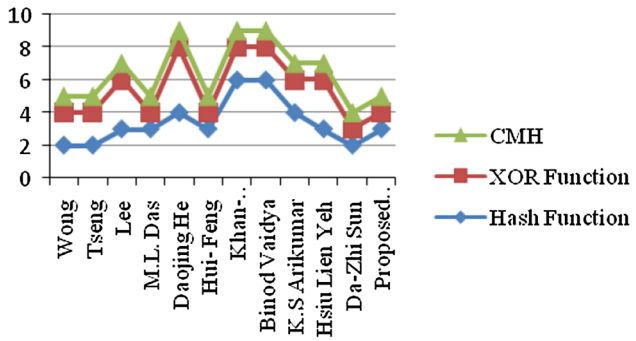

Fig. 3 Login phase for protocols

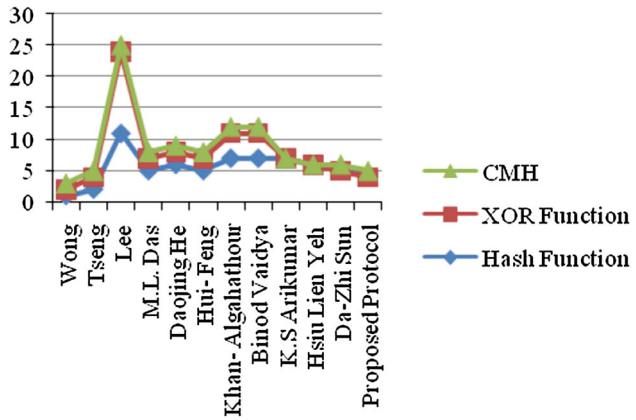

Fig. 4 Authentication phase for protocols

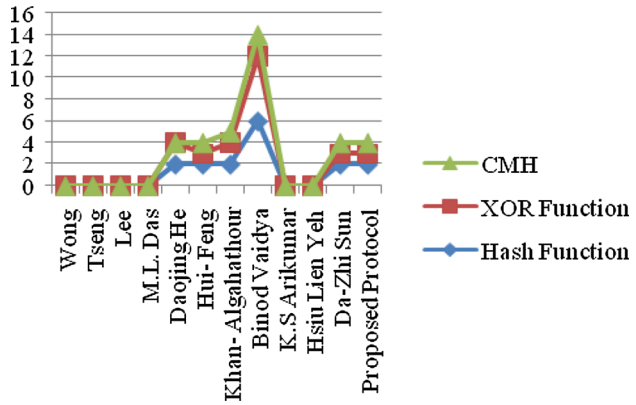

Fig. 5 Password change phase for protocols

Our security framework can effectively defend against the Sybil attack, the node replication attack, and the wormhole attack by including the security time stamp in our protocol, a new node is only allowed to join the sensor network during its time stamp length. After that it becomes an old node. Hence, malicious ''new'' nodes are prevented from joining the sensor network at the very beginning, because they do not have the proper bootstrapping time,

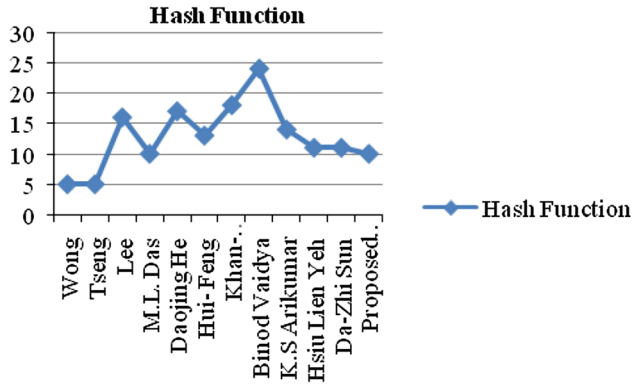

Fig. 6 Total hash function for protocols

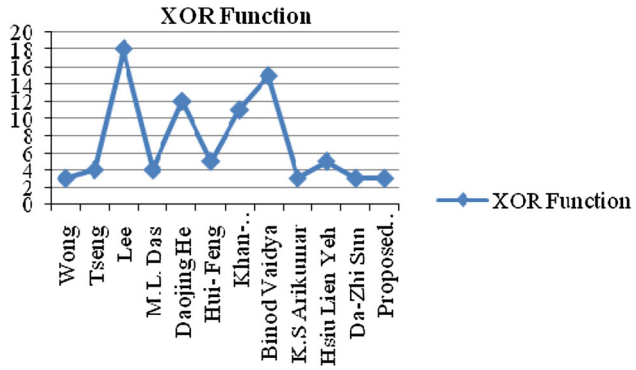

Fig. 7 Total XOR function for protocols

and they are prevented from falsifying the latest security time stamp which does not match their certificates. The comparative study chart is as shown in Table 2 shows the proposed framework has less computational cost and overhead as compare to the respective other protocol.

5 Conclusion and future work

In this paper we analyze the security authentication scheme for wireless sensor networks and proposed a authentication protocol to defend against malicious attack. The proposed scheme justifies the security analysis. We are heading towards a future of miniaturization and wireless connectivity, where in sensor networks have the ability to deliver both at exceedingly low cost. For future research, we propose extending a secured mechanism to include trust establishment and trust management with confidentiality in sensor networks. Besides, this we have an interest in exploring and solving security issues in security and information assurance, and protection against identity theft and wish to implement the proposed scheme for better access control in WSN.

References

1. Chen JH, Salim MB, Matsumoto M (2011) A single mobile target tracking in Voronoi-based clustered wireless sensor network. J Inf Process Syst 7(1):17–28
2. Kumar D, Aseri TC, Patel RB (2011) Multi-hop communication routing (MCR) protocol for heterogeneous wireless sensor networks. Int J Inf Technol Commun Converg 1(2):130–145
3. Jeong YS, Lee SH (2006) Secure key management protocol in the wireless sensor network. J Inf Process Syst 2(1):48–51
4. Wong CK, Gouda M, Lam S (2000) Secure group communications using key graphs. Proc IEEE Trans on Netw 8(1):16–29
5. Sun DZ, Li JX, Feng ZY, Cao ZF, Xu GQ (2013) On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Pers Ubiquitous Comput 17(5):895–905
6. Sharifi M, Ardakani SP, Kashi SS (2009) SKEW: an efficient self key establishment protocol for wireless sensor networks. In: Proceeding of IEEE 2009, p. 250–257
7. Holohan E (2010) Authentication using virtual certificate authorities: a new security paradigm for wireless sensor networks. In: Proceeding of Network Computing and Applications (NCA), IEEE 2010, p. 92–99
8. Jiang C, Li B, Xu H (2007) An efficient scheme for user authentication in wireless sensor networks. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007
9. Tseng HR, Jan RH, Yang W (2007) An improved dynamic user authentication scheme for wireless sensor networks. In: Proceedings of IEEE Globecom, Washington, DC, p. 986–990
10. Ko LC (2008) A novel dynamic user authentication scheme for wireless sensor networks. IEEE ISWCS 2008, p. 608–612
11. Benenson Z, Gartner F, Kesdogan D (2004) User authentication in sensor networks. In: Proceeding Workshop Sensor Networks, Lecture Notes Informatics Proceedings Informatik, 2004
12. Arikumar KS, Thirumoorthy K (2011) Improved user authentication in wireless sensor networks. In: Proceedings of ICETECT 2011, p. 1010–1015
13. Das ML (2009) Two-factor user authentication in wireless sensor networks. IEEE trans on wirel commun 8(3):1086–1090
14. Huang HF, Chang YF (2010) Enhancement of two factor user authentication in wireless sensor network, in sixth international conference on intelligent information hiding and multimedia signal processing, 2010 IEEE. p. 27–30
15. Vaidya B, Makrakis D, Hussein T (2010) Improved two-factor user authentication in wireless sensor networks Second International Workshop on Network Assurance and Security Services in Ubiquitous Environments IEEE-2010, pp 600–606
16. he D, gao Y, chan S, chen C, bu J (2010) An enhanced two-factor user authentication scheme in wireless sensor networks. Adhoc Sens Wirel Netw 0:1–11
17. Khan MK, Alghathbar K (2010) Cryptanalysis and security improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'. Sensors 10(3):2450–2459
18. Yeh HL, Chen TH, Liu PC, Kim TH, Wei HW (2011) A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors 11:4767–4779
19. Sarika T, Nawaz SS (2011) Multi-factor user authentication in wireless sensor networks. Int J Comput Sci Telecommun 2(6):59–63