www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12069-12075

An Efficient Authentication Scheme for Wireless Sensor Network

Alok Kumar[1], Akhilesh Yadav[2]

[1]Department of computer science & engineering, Babu Banarasi Das University,
Lucknow, 226028, Uttar Pradesh, India
alokmind@gmail.com

[2]Department of computer science & engineering, Babu Banarasi Das University,
Lucknow, 226028, Uttar Pradesh, India
Akhi2232232@gmail.com

Abstract: ***Sensor nodes are usually installed in public or unattended environment and secure authentication scheme performs important role among communication in between user, wireless sensor network (WSN) and sensor node as it secures the communication by sweeping the security flaw. Authentication scheme must be developed by using all possible available resources and without compromising any security flaw/risk. This paper proposes an efficient authentication scheme for wireless sensor network, which is based on username password and smart card, and this scheme provides better security in between communicating nodes. Users are able to choose own username and password. This scheme involves registration, login and session key establishment phase. Most of scheme don't allow to hide username in entire scheme, which may lead to insider attack. This scheme uses the combination of symmetric and asymmetric keys, and maintains the authenticity of nodes using mutual authentication that prevents the network from man-in-middle attack and makes it more secure against other security attacks such as insider attack, password guessing attack, replay attack etc.***

Keywords: Authentication protocol, smartcard, wireless sensor network, mutual authentication.

1. Introduction

A wireless sensor network is active collection of sensor nodes of several hundred and even thousand, and base station, these sensor nodes have the some limited capabilities such as memory, data processing, power sources, and radio signal transmission range [16], [17]. All these capabilities are depends upon the physical condition of the environment and with hardware limitations. These sensor are able to sense the physical and environment condition of the entity such as pressure, temperature, humidity and sounds etc. and they are mostly deployed in hostile or unattended environment such as battlefield, top of the tower and mountains, on international border's site to track the border's live activity and used in home security to detect the intruder etc. Sensor sense these data and transfer to the gateway node (GWN). Gateway node works as a base station for users and sensor nodes, and also works as a network administrator, which authenticates and authorizes the user and sensor node to use resources of the WSN. Sensor node sends the data to GWN and GWN processes the data stores the information in its database for user and other related tasks.

ID and password based authentication scheme are normally used for authentication purpose. Smart card based authentication scheme can ensure better security in electronic based applications in between communicating nodes. The combination of password and smart card based scheme is suitable for authentication in wireless sensor network. Many schemes are proposed for this type of network, but those implementations are for authentication purpose only, and do not ensure the security of network's entities and resources.

As we know, sensor may deploy in unattended environment, so attacker may physically alter the active sensor node and may capture it and steal the sensitive data from it. Due to the invisibility of the radio network, attacker can easily eavesdrop the network traffic and may intercept in its activity. So the special care is require to protect the user's and data's security.

2. Related work

A remote user authentication scheme was proposed by Hwang-Li [10], and it works with timestamp and public key cryptography. This scheme prevents the replay attack and it does not maintain the password table to verify the login users. There is a secret key to compute the user's password. This scheme take the advantages of mathematical problem discrete logarithm over finite fields. So it is difficult to compute the secret key to the attacker, it can be done by legitimate user only.

Two-factor user authentication was proposed by Das [3], and it is simple remote user authentication scheme based on password and smart card. It minimize the computational complexity using

XOR and hashing. This scheme does not have mutual authentication, so it faces some security problem such as node compromising attack and password guessing attack by attacker showed by Khan and Alghathbar [11]. At sensor node side, attacker can capture the node and base station cannot find that attack. Later, Some author proposed their scheme based on two factor user authentication schemes with mutual authentication, Li et al. [5] proposed a secure billing service using Das' scheme, Das et al. [8] proposed a dynamic password based user authentication scheme, and Yeh et al. [7] proposed user authentication scheme based on elliptic curve cryptography (ECC) that overcome all the security flaw of the Das [3] scheme.

Ramasamy and Muniyandi [2] suggested a simple authentication scheme for smart card using public key cryptography of RSA key pair. As they declare his scheme is secured against parallel session attack, smart card lost attack, and DOS attack, but it do not protect the network through replay attack. Watro et al. [12] proposed a user authentication scheme, which is based on public key cryptography using RSA [14] and Diffie Hellman [13]. This scheme suffers from the sensor node capturing attack for the new user. It is computationally costly, and it has no mutual authentication. Wong et al. [15] suggested a user authentication scheme too, and it is based on password and cryptographic hash function. It has some serious security flaws like many logged in users' attack which can be performed by insider with the same username.

Kumar [6] proposed a scheme in which user and server authenticates each other, and generates a secure secret session key for secure communication. This scheme also provide the power to update the password freely. Later, Kumar [9] update his previous scheme with new remote user authentication scheme. It too provide mutual authentication with message confidentiality. According to Kumar his scheme is secured against replay and stolen verifier attack. User can easily change the related password without communicating any server.

In 2013, Xue et al. [4] suggested a temporal credential based mutual authentication and key agreement scheme that provide high security and more feature in very low cost and low computation time. As Xue et al. titled that their scheme is secure against many security flaw, but Li et al. [1] proved that it some serious security flaw such as, it can't restrict stolen verifier and insider attack, offline password guessing attack, lost smart card problem, and many logged in users' problem.

3. Proposed Scheme

Symbols	Description
U_i	i^{th} User
S_j	j^{th} Sensor node
URC	Unique Registration Code
X_1	A Secret key generated by user
GWN	Gateway node
ID_i/PWD_i	User identity/Password of the user
SID_j/SK_j	Sensor identity/sensor key
V_1/V_2	Are the user/sensor verifier
K_{GWN_U}/K_{GWN_S}	Private system keys only know to GWN
GC_i/GC_j	Credential issued by GWN to user/sensor
KEY_{ij}	Shared session key between user and sensor
TS	The timestamp value
TE_i	Validity of user's login
K_i/K_j	A random key of user/sensor
$\oplus$	The bitwise exclusive-OR operation
$H(\bullet)$	The one-way hashing function
$\|\|$	The bitwise concatenation operation

Table 1: Notation used throughout this paper

This paper proposes an efficient Authentication scheme for WSN. Which uses the smart card and password and authenticates through one way hash functions. It has two phase, registration phase, and login and key establishment phase. Complete scheme are explained below.

3.1 Registration Phase

This phase is explained in two parts, user registration and sensor node registration.

3.1.1 User registration

At the time of user registration GWN shares a unique registration code (URC) with user.

- U_i chooses his ID_i and password PWD_i and compute $H_1(ID_i)\|","\|H_1(PWD_i)$, and encrypt it with URC through advance encryption standard (AES-256) and compute $A_1 = URC(H_1(ID_i)\|","\|H_1(PWD_i))$. Similarly computes $A_2 = H_1(H_1(ID_i)\|X_1)$ and sends $\{A_1, A_2, TS_1\}$ to the GWN. Where TS_1 is the current time stamp value.
- As GWN receives these values, it checks the validity of the timestamp $|T_{GWN}-TS_1|<\Delta T$, where T_{GWN} is the current timestamp value of the GWN, and ΔT is the expected time of transmission delay. If timestamp not validate then GWN reject the U_i's registration request. Otherwise, GWN decrypt A_1 messages and compute $H_1(ID_i)$ and $H_1(PWD_i)$, if get success means message is from legitimate user. Now GWN computes a gateway credential $GC_i = H_1(K_{GWN\_U}\|ST_i\|M_i)$, $M_i = H_1(ST_i\|H_1(ID_i)\|H_1(PWD_i))$, $V_1 = H_1(Zi\oplus H_1(H_1(ID_i)\|H_1(PWD_i))$, $PGC_i = GC_i\oplus Z_i$ and $Z_i = H_1(H_1(ID_i)\|X_1))$. Now GWN personalize a write protected smart containing $[H_1(.), H_2(.), H_3(.), V_1, M_i, PGC_i, Z_i]$ and sends to U_i
- U_i receives a smartcard and verifies the smart card by computing $Z_i^* = H_1(H_1(ID_i)\|X_1))$ and then calculates $V_1^* = H_1(Z_i\oplus H_1(H_1(ID_i)\|H_1(PWD_i))$, if $V_1^* = V_1$ then U_i accepts the smartcard and enters his secret key value X_1 to activate

the smartcard [$H_1(.)$, $H_2(.)$, $H_3(.)$, V_1, M_i, PGC_i, Z_i, X_1]. Now U_i does not need to remember the value of X_1.

- And GWN maintains a session table that is shown below.

USER ID	Status record	Last login	Service time
$H_1(ID_i)$	(1,0)	…	ST_i

Table 2: session table maintained by GWN

3.1.2 Sensor Node Registration

Sensor node has some pre-shared values with GWN $H2(SID_j||SK_j)$ and $H2(SID_j)$ and GWN also knows about SID_j and SK_j.

- S_j computes $B_1 = H_2(H_2(SID_j||SK_j)||TS_2)$ and $B_2 = H_2(H_2(SID_j)||TS_2)$ and sends the registration message {B_1, B_2, TS_2} to the GWN.
- After receiving the registration request GWN first check the validity of timestamp $|T_{GWN}-TS_2|<\Delta T$, if TS_2 doesn't validates then GWN rejects the registration request of sensor node. Otherwise, computes $B_1^* = H_2(H_2(SID_j^*||SK_j^*)||TS_2)$ and $B_2^* = H_2(H_2(SID_j)^*||TS_2)$ if $B_1^* = B_1$ and $B_2^* = B_2$ If true, that means S_j is the legitimate node then GWN Calculates $V_2 = H_2(H_2(SID_j||SK_j)||TS_3)$, $GC_j = H_2(K_{GWN\_S}||H_2(SID_j||SK_j))$ and $PGC_j = GC_j \oplus H_2(H_2(SID_j)||TS_3)$. Now GWN sends the registration message {V_2, PGC_j, TS_3} to sensor node.
- After receiving the GWN's message, S_j checks $|T_j-TS_3|<\Delta T$, if TS_3 doesn't validates then sensor S_j rejects the message of GWN. Otherwise, S_j computes $V_2^* = H_2(H_2(SID_j||SK_j)^*||TS_3)$, if $V_2^* = V_2$ then it calculates $GC_j = PGC_j \oplus H_2(H_2(SID_j)||TS_3))$ by using PGC_j, and stores the GC_j.

Registration phase

User (U_i) — **Gateway Node (GWN)**

URN //unique registration code

$A_1 = URC(H_1(ID_i)||","||H_1(PWD_i))$, $A_2 = (H_1(ID_i)||X_1)$,

- GWN checks the timestamp validity
- Decrypt the both messages
- if success then calculate-
- $GC_i = H_1(K_{GWN\_U}||ST_i||M_i)$
- $M_i = H_1(ST_i||H_1(ID_i)||H_1(PWD_i))$
- $V_1 = H_1(Z_i \oplus H_1(H_1(ID_i)||H_1(PWD_i))$
- $PGC_i = GC_i \oplus Z_i$
- $Z_i = H_1(H_1(ID_i)||X_1))$
- And personalize the smart card with
- [$H_1(.)$, $H_2(.)$, $H_3(.)$, V_1, M_i, PGC_i, Z_i]

Smart card to User

- User calculate $Z_i^* = H_1(H_1(ID_i)||X_1))$
- Compute $V_1^* = H_1(Z_i^* \oplus H_1(H_1(ID_i)||H_1(PWD_i))$
- Compare $V_1^* = V_1$ if true then
- User accepts that card and enters his secret value of X_1 to activate the card [$H_1(.)$, $H_2(.)$, $H_3(.)$, V_1, M_i, PGC_i, Z_i, X_1] to use

// Now user does not need to remember the value of X_1

Gateway Node (GWN) — **Sensor Node (S_j)**

SID_j and SK_j are Pre shared

- $H2(SID_j||SK_j)$
- $H2(SID_j)$

$B_1 = H_2(H_2(SID_j||SK_j)||TS_2)$, $B_2 = H_2(H_2(SID_j)||TS_2)$,

- GWN checks the validity of time stamp
- Compute $B_1^* = H_2(H_2(SID_j^*||SK_j^*)||TS_2)$
- And $B_2^* = H_2(H_2(SID_j)^*||TS_2)$
- Compare $B_1^* = B_1$ And $B_2^* = B_2$
- If true then calculate-
- $V_2 = H_2(H_2(SID_j||SK_j)||TS_3)$
- $GC_j = H_2(K_{GWN\_S}||H_2(SID_j||SK_j))$
- $PGC_j = GC_j \oplus H_2(H_2(SID_j)||TS_3)$

V_2, PGC_j, TS_3

- checks the timestamp validity
- Calculate $V_2^* = H_2(H_2(SID_j||SK_j)^*||TS_3)$ if $V_2^* = V_2$ true then
- Calculate GC_j by using PGC_j -
- $GC_j = PGC_j \oplus H_2(H_2(SID_j)||TS_3))$

Table 3: Registration Phase

3.2 Login and Key Establishment Phase

In this phase U_i login into the server and trying to access sensor node. Note: at any time GWN rejects the any message coming from U_i's side then immediately GWN increase the first value of status record of the session table by +1 and up to 2.

- When U_i wants login, then U_i inserts a smartcard into the login or card terminal and enters ID_i and PWD_i and login terminal computes $Z_i^* = H_1(H_1(ID_i)||X_1))$ and Calculates V_1^* and compares with stored V_1, If $V_1 = V_1^*$ true means U_i is successfully verified then computes further $GC_i = PGC_i \oplus Z_i$, $CID_i = H_1(V_1||TS_4) \oplus GC_i)$ and $USK_i = K_i \oplus (GC_i||TS_4||H_1(ID_i))$. Where K_i is the random secret key,

and sends a login message $\{H_1(ID_i), CID_i, USK_i, M_i, TS_4\}$ to GWN.

- GWN receives the login message and check the validity of timestamp $|T_{GWN}-TS_4|<\Delta T$, if not true, GWN terminates the current session. Otherwise, GWN computes $M_i^* = H_1(ST_i\|H_1(ID_i)\|H_1(PWD_i))$ and Compare $M_i^* = M_i$ with stored value of M_i, if true then further Computes $GC_i^* = H_1(H_1(K_{GWN\_U}\|ST_i\|M_i^*)$ and also computes $CID_i^* = H_1(V_1^*\|TS_4)\oplus GC_i^*)$ and Check for $CID_i^* = CID_i$ if true then U_i successful validate the login and GWN update the session table that is shown below.

USER ID	Status record	Last login	Service time
$H_1(ID_i)$	(1,1)	TS_4	ST_i

Table 4: updated session table maintained by GWN

- Now GWN chooses a appropriate sensor node for next communication step and Computes $K_i = USK_i\oplus H_1(GC_i\|TS_4\|H_1(ID_i))$, $VID_{GWN} = H_1(ID_i)\oplus H_2(GC_j\|TS_5)$, $CID_{GWN} = H_2(H_1(ID_i)\|GC_j\|TS_5)$ and $USK_{GWN} = K_i\oplus H_2(GC_j\|TS_5\|H_2(SID_j))$, and GWN sends the message $\{VID_{GWN}, CID_{GWN}, USK_{GWN}, TS_5\}$ to S_j.
- S_j receives the message and checks the validity of timestamp $|T_j-TS_5|<\Delta T$, if not true, GWN terminates the current session. Otherwise, accepts the message and Calculate $H_1(ID_i)^* = VID_{GWN}\oplus H_2(GC_j\|TS_5)$, $CID_{GWN}^* = H_2(H_1(ID_i)^*\|GC_j\|TS_5)$.
- Compare $CID_{GWN}^* = CID_{GWN}$ if true, that means messages source is genuine then Compute U_i's secret key $K_i = USK_{GWN}\oplus H_2(GC_j\|TS_5\|H_2(SID_j))$, and S_j chooses own secret key K_j and calculates $CID_j = H_2(H_2(SID_j)\|H_1(ID_i)\|K_j\|TS_6)$ and $USK_j = K_j\oplus H_2(K_i\|TS_6\|\|H_1(ID_i))$. Now S_j sends a message $\{H2(SID_j), CID_j, USK_j, TS_6\}$ to both U_i and GWN.

Both U_i and GWN receives the S_j's message and checks the validity of timestamp $|T_j-TS_6|<\Delta T$, if not true, GWN immediately terminates the current session. Both U_i and GWN Compute $CID_j^* = H_2(H_2(SID_j)\|H_1(ID_i)\|K_j\|TS_6)$, If $CID_j^* = CID_j$ true, that means message is genuine and then compute S_j's secret key $K_j = USK_j\oplus H_2(K_i\|TS_6\|\ H_1(ID_i))$ and finally both GWN and U_i compute a shared secret key $Key_{ij} = H_3(k_i\oplus K_j)$ for future secure communication between user and sensor.

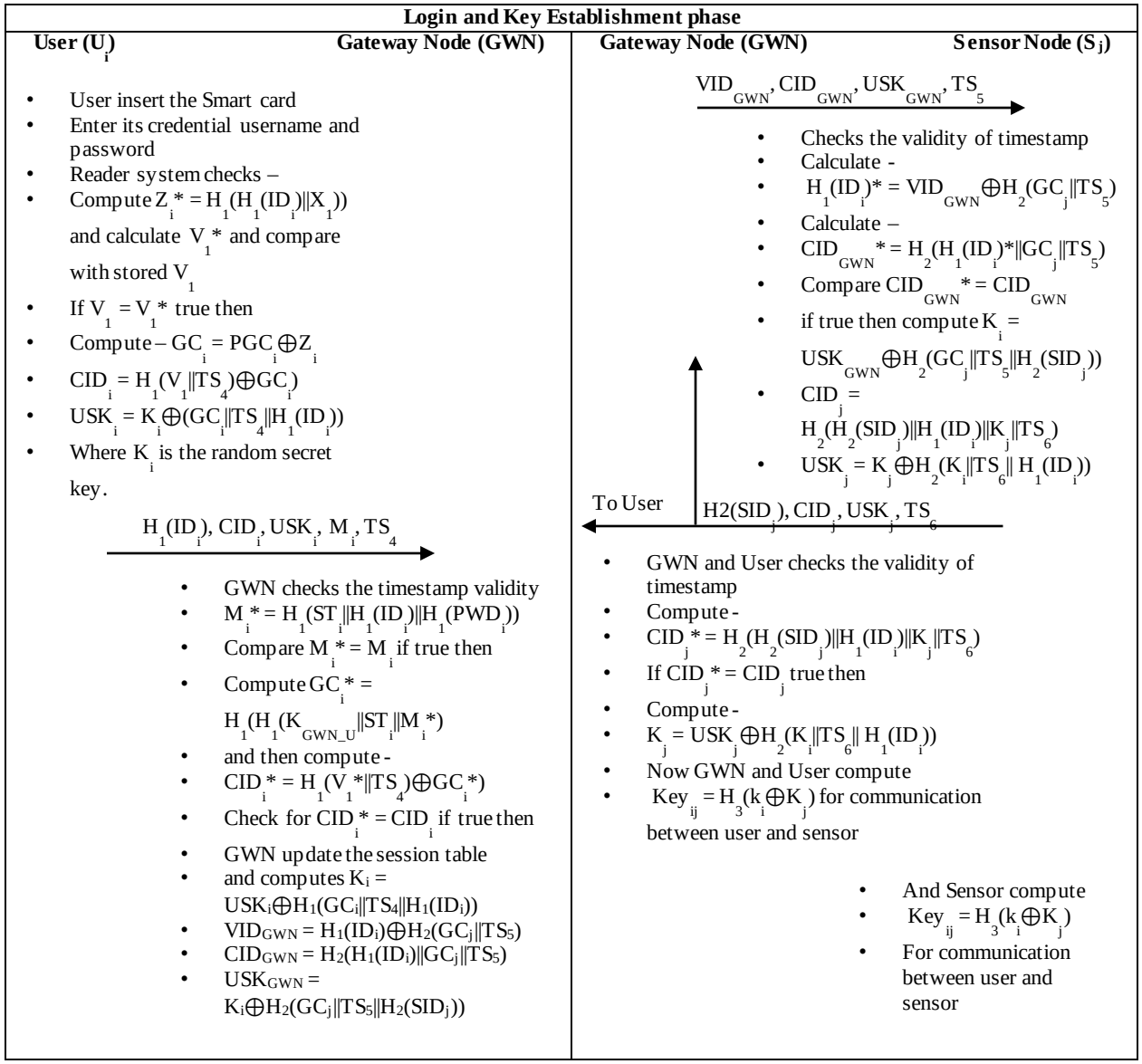

Table 5: Login and key establishment phase

4. Security Analysis of Proposed Scheme

4.1 Offline password guessing attack and stolen verifier attack

This attack is impossible in practice. Let the scenario, if attacker eavesdrop the any message like user's verifier $V_1 = H_1(H_1(H_1(ID_i)\|X_1)) \oplus H_1(H_1(ID_i)\|H_1(PWD_i))$ from the running network and try to retrieve userid (ID_i) and password (PWD_i) from it, which contains user's complete credential. X_1 is the user's secret key and not revealed to GWN too. Size of X_1 is large about 160 bit. The probability to retrieve exact value of X_1 is $½^{160}$, it is likely to impossible. Attacker also can't retrieve the any user's credential because all the traffic over the network is secured with SHA-256 and 2^{256} calculations are required to break it. It is infeasible computing in practice. Let if attacker steals the user's userid and password by seeing the live login process then attacker must also require smartcard that is impossible.

4.2 Active parallel session attack

This scheme allows only one active session from user. No one can login multiple session on the legitimate servers. GWN maintains a session table, which contains the U_i's session information and maintain one session in same time. Session table contains records in the form of status record (0,0). Where first value can be up to "2" from "0", which records the unsuccessful login attempts. And second value can be either "0" or "1" only. Where 0 shows U_i is not login or session is not

established and 1 shows the U_i active session. So here this scheme is protected from this attack.

4.3 Smart card lost problem

Let anyhow, attacker get the smart card and try to steal information from it. Note smart card is write protected attacker can't write anything in it. All the credential are secured with hash and card is locked with userid ID_i and Password PWD_i then it is impossible to guess correct both ID_i and PWD_i together. Means, this scheme is protected from smart card lost problem.

4.4 Insider attack

In this scheme no message is in plain text. All messages are secured with hash. This scheme uses digested $H_1(ID_i)$ and $H_1(PWD_i)$. It is easy to get $H_1(ID_i)$ and $H_1(PWD_i)$ for insider, but insider can't retrieve or find the real credential because no communication message contains real identity (ID_i and PWD_i) of any user. Therefore insider attack not possible on this scheme.

4.5 Replay attack and man-in-middle attack

As this paper shows, this scheme is secured from stealing user's credential. Let if attacker eavesdrop the network messages and try to push again those messages in to the network to get login new active session. In this scheme each and every communicating messages are secured with timestamp, and receiver always check the validity of timestamp using $|T_{GWN}-TS_4|<\Delta T$, where T_{GWN} is the receiver's timestamp and TS_4 is the sender's timestamp. If it ($|T_{GWN}-TS_4|<\Delta T$) is not true then receiver immediately terminates the session and rejects the sender's message. Let attacker eavesdrop the login message ($H_1(ID_i)$, CID_i, USK_i, M_i, TS_4) and let anyhow attacker convince the receiver that sender's timestamp is valid that means $|T_{GWN}-TS_4^*|<\Delta T$, where TS_4^* is the sender's altered timestamp accepted by GWN. In next step, GWN compute CID_i^* which uses sender's real timestamp and GWN won't be able to compute $CID_i^* = CID_i$ and rejects the message because of it is impossible to alter timestamp in CID_i and both genuine communicating entities authenticates each other. There for replay and man-in-middle attack are not possible in this scheme.

4.6 Mutual authentication

Mutual authentication is the advantage of this scheme, in which both communicating entities authenticates each other that prevents user from man-in-middle attack. As in registration phase of user. U_i sends a registration message $\{A_1, A_2, TS_1\}$ to the GWN and this message is computable by GWN only. After computing GWN issue a smart card to user. User receives a smartcard and verifies it through $V_1^* = H_1(Z_i \oplus H_1(H_1(ID_i)\|H_1(PWD_i)$. This V_1^* can be computable by legitimate user only. If U_i get success to compute V_1^* and successfully compares $V_1^*=V_1^*$ then user accepts the smartcard and enters his/her secret value X_1 to activate the smartcard.

4.7 Masquerade attack

In the first registration step GWN shared a secret unique registration code (URC) to valid user only. So no user can register himself/herself to GWN without URC. Therefore this scheme also secured from this attack.

5. Performance analysis

Performance in the terms of computational cost of the scheme in different phases (registration, login and key establishment phase etc.) and compare with other schemes. Here computational cost is measured through encryption technique and digest algorithm. Some operation such as XOR and concatenation things are not measured. In the notations T_H defines the computation time of hash, T_{AES} time to take AES encryption, T_{ECC} time to take ECC encryption. Some related scheme's comparison are shown in table 5. Scheme of Ramasamy and Muniyandi [2] uses RSA and takes $8T_{MMUL}$ and $7T_{MEXP}$, where T_{MMUL} is the time taken for a modular multiplication and T_{MEXP} is time taken for modular exponentiation. Kumar's [6] scheme uses $6T_{MEXP} + 2T_{Ck} + 3T_H$, where T_{Ck} is the time taken to execute a function for checking the digit of registered users. Another of kumar's [9] scheme uses $4T_{MEXP} + 2T_{Ck} + 2T_H$. Time of hash is faster than ECC, SHA-256 takes average 0.0002 seconds and ECC takes average 0.6 seconds on the normal home computer.

Phases	Watro et al.	Das	Wong et al.	Khan and alghathbar	Li et al. [1]	Yeh et al.	Xue et al.	Our proposed scheme
Registration, login and authentication	$3T_{PU} + 3T_{PR} + 2T_H$	$12T_H$	$7T_H$	$14T_H$	$26T_H$	$8T_H + 8T_{ECC}$	$43\ T_H$	$44\ T_H + 1\ T_{AES}$

Table 6: Performance comparison of our scheme with other related scheme on the basis of computation cost.

6. Conclusion

In this paper, we proposed a secured authentication scheme for WSN. The proposed scheme restricts many of well-known attacks efficiently. The proposed scheme uses lightweight one way hash SHA-256, which works well and provide good security to the network entities and reduces the computation cost. Mutual authentication is the good part of the scheme that makes this scheme more secure by preventing from man-in-middle attack. Our advance scheme has another good functionality that scheme don't uses the user's identity (U_i) in

original form, it uses the hash value of identity, which prevents the scheme from insider attack. Our scheme is very good for WSN in practice.

References

[1] Li, C.T.; Lee, C.C.; Weng, C.Y, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor network," Sensor Journal, 13, 9589-9603, 2013.

[2] Ramasamy, R.; Muniyandi, A.P, "An efficient password authentication scheme for smart card," Int. J. Netw. Secur. 14, 180–186, 2012.

[3] Das, M.L, "Two-factor user authentication scheme in wireless sensor networks," IEEE Trans. Wirel. Commun. 8, 1086–1090, 2009.

[4] Xue, K.; Ma, C.; Hong, P.; Ding, R. "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," J. Netw. Comput. Appl. 36, 316–323, 2013.

[5] Li, C.T.; Lee, C.C.; Wang, L.J.; Liu, C.J. "A secure billing service with two-factor user authentication in wireless sensor networks," Int. J. Innov. Comput. Inform. Contr. 7, 4821–4831, 2011.

[6] M. Kumar, "An enhanced remote user authentication scheme with smart card," International Journal of Network Security, vol. 10, no. 3, PP. 175-184, 2010.

[7] Yeh, H.L.; Chen, T.H.; Liu, P.C.; Kim, T.H.; Wei, H.W. "A secure authentication protocol for wireless sensor networks using elliptic curves cryptography," Sens. J. 11, 4767–4779, 2011.

[8] Das, A.K.; Sharma, P.; Chatterjee, S.; Sing, J.K. "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," J. Netw. Comput. Appl. 35, 1646–1656, 2012.

[9] M. Kumar, "A new secure remote user authentication scheme with smart cards," International Journal of Network Security, vol. 11, no. 3, PP. 128-133, 2010.

[10] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on consumer Electronics, vol. 46, no.1, pp. 28-30, 2000.

[11] Khan, M.K.; Alghathbar, K. "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," Sensors Journal, 10, 2450–2459, 2010.

[12] RonaldWatro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. "Tinypk: securing sensor networks with public key technology," In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pages 59–64. ACM, 2004.

[13] Whitfield Diffie and Martin Hellman. "New directions in cryptography," Information Theory,IEEE Transactions on, 22(6), 644–654, 1976.

[14] Ronald L Rivest, Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21(2):120–126, 1978.

[15] Kirk HM Wong, Yuan Zheng, Jiannong Cao, and Shengwei Wang. "A dynamic user authentication scheme for wireless sensor networks," In Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006, IEEE International Conference on, volume 1, pages 8–pp. IEEE, 2006.

[16] Asadi, M.; Zimmerman, C.; Agah, A. "A game-theoretic approach to security and power conservation in wireless sensor networks," Int. J. Netw. Secur. 15, 50–58, 2013

[17] Mi, Q.; Stankovic, J.A.; Stoleru, R. "Practical and secure localization and key distribution for wireless sensor networks," Ad Hoc Netw. 10, 946–961, 2012.

Author Profile

Alok Kumar received the B.Tech degree from J.S. Institute of management & Technology shikohabad, affiliated to uttar pradesh technical university and pursuing M.Tech from Babu Banarasi Das University Lucknow.

Akhilesh Yadav received his M.Tech degree from Babu Banarasi Das University Lucknow and now he is an assistant lecturer in same university.