International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 37584-37586

Trust based secure information exchange between user and sensor node using authentication method and verified at each gateway node in wireless networks

D. SRUJAN CHANDRA REDDY,
Professor, Department of Computer Science and Engineering,
PBR VITS, Kavali, Andhra Pradesh India -524201
srujand@hotmail. com

V. V. SUNIL KUMAR,
Professor, Department of Computer Science and Engineering
PBR VITS, Kavali, Andhra Pradesh India -524201
sunil. vemula1981@gmail. com

Abstract
Day to day usage of wireless network is increased rapidly. A wireless communication between user and sensor node may not be authenticated may be attacker is reside on gateway node and try to retrieve the confidential data from both parties and after hacking information force attacks. In this paper we proposed a new method of mutual authentication method using temporal credential values to protect from attacks. In our method user and sensor nodes must registered with gateway node before start communication and gateway node issue smart values to both user and sensor node with a period of validity. We have done cryptanalysis on earlier methods and we come to know that still there is a possibility of forcing attacks. At the end we discussed how our method is protecting from different attacks when compared with earlier method.

Keywords: Wireless communication, Sensor node, Gateway node, Mutual authentication, Security attacks

I. Introduction

In wireless network a huge number of sensor nodes are involved in the communication. The nodes like user node, sensor node, base station, gateway node present in the communication. In general by considering the growth and use of internet for information sharing all these nodes must be active participants to send or receive confidential data. Now days the users who are using smart wireless phones are very much interested to use internet applications to reduce their time of shopping which leads the problem of secure wireless communication or channel. The sensor nodes that are involving in the communication may be knowing or unknowing using gateway nodes in their communication. When gateway node is participating in the communication is their chance to attacker hidden in the gateway node, monitor the traffic of communication between to users and try to force attacks.

Protecting data in gateway node is a one of the challenging issue. Our main objective is to protect information at gateway node from various security attacks. We proposed an authentication method where the user and all sensor nodes must be registered with gateway node and gateway node after verification issue temporal credential with a period of validity. We applied cryptanalysis on earlier method and in our proposed method we resolved attacks which are possible in the existing method.

Rest of the paper organized as, in section II we explained background work, in section III we discussed the proposed method, we elaborate in section IV how our proposed method protect from various attacks which are faced by previous method.

II. Literature Survey

The authors in [1] presented a password authentication method using simple functions like one way hashing technique, XOR operations for wireless sensor networks and their scheme provides password based authentication. The authors in [2] proposed mathematical two factor user authentication for wireless networks to secure exchange of session key and applied cryptanalysis on [1] and they proved that method [1] still possible to vulnerable like forgery attack and masquerade attack. Authors [2] proved that their method protects from replay attack, stolen verifier attack, masquerade attack and password guessing attack. Authors [2] also proved that method which is provided by authors [7] is possible to access multiple users with same user id.

The researchers in [3] proposed new method of mutual authentication between users, gateway and sensor node over wireless network. They compare their results with method [2] when the power consumption is same in both methods is same method [3] shown better results then [2]. But unfortunately the authors in [3] proved that method which is proposed by authors [2] is fails to achieve mutual authentication. The researchers in [4] described a new method of mutual authentication, they proved that their method is useful to solve some of serious issues faced by method [2], for example frequent password change or update is not possible, fail to provide mutual authentication between user and gateway or gateway and server and there is a chance to force bypassing attack.

The authors in [5] proposed elliptical curve cryptography based mutual authentication to solve the weakness their in [2]. The authors in paper [6] proposed mutual authentication

method based on temporal credentials, in their scheme gateway node issues temporal credential to both user and sensor node and in their method key management method is used. In this paper we proposed mutual authentication key management method based on temporal credentials, temporal credentials are issued by gateway node with time period to both user and sensor node, and if the time period reaches expiry gateway node re issue temporal credentials after verifying the user.

III. Proposed Method

List of notations used in the proposed system.
Ui → ith user
IDi→user Ui ID.
SIDj→Sensor node ID.
Pi → the password of user Ui.
G → Gateway node
p, q → Gateway node assigns secret values to user Ui and server V
ETi→ Temporary credentials of user Ui
r → random value selected by user Ui
t → random value selected by sensor node V
u → temporal value for sensor node V
h(.)→ hash function
⊕ → Bitwise exclusive OR function
|| → Concatenation

In our proposed method user U_i validated at three stages and they are registration stage, login stage, and authentication stage.

i. Registration Stage

In this stage we are using two methods one is for user U_i and the other one is for sensor node. The ID and password hash value of both user and sensor node is stored at gateway node database and these values are used by gateway node when the user and sensor node wants to communicate with each other.
Step 1: User calculate password $UP_i = h(r \| P_i)$ and at time stamp T1user U_i send request message (ID_i, UP_i, T_1) to gateway node G through secure way.
Step 2: after receiving request from user Ui at time T2 then G verifies that is it T2-T1 > Δt, if it is the case then G simply reject user request or otherwise user is verified by getting h(Pi) from gateway node database using IDi and then calculate new password UPNi = h(r || h(Pi)) and verifies if both password is same then user is allowed to proceed further by calculating following calculations or otherwise user is rejected.

A= h(T1||T2||ETi||UPi)
B=h(IDi||p||ETi)
C=B⊕h(r||T2||ETi)
IDi*=IDi⊕h(ETi||T1||T2||B)

The gateway node G stores values ETi⊕h(u||p), IDi*⊕r⊕h(p), T2 ⊕ h(p⊕u), T1⊕ h(p||u) into database.
Step 3: By using secret channel gateway node G issued smart card to user which contain values (IDi*, h(IDi)⊕T1, ETi, C, h(T1)⊕T2).
Step 4: Each sensor node Vi in the network is assigned unique ID called VID_i and each sensor node must be register with gateway node and its password SP_i.
Step 5: Sensor node Vi selects a random number t, calculate D= t⊕h(SPi), UPi = h(t||h(SPi)) and send request to gateway node G (VID_i, UP_i, D, T_3).
Step 6: After receiving sensor node registration request at T4, gateway node verifies that T4-T3> Δt true or not, if it is true then immediately sensor registration request refused or otherwise calculations further proceed to authenticate sensor node.
Step 6. 1: Gateway node get the value of h(SPi) from database by indexing its identity, calculate D⊕h(SPi) = t, UPN_i = h(t|| h(SPi)), verifies that UPN_i is equal to UP_i and if it is same user is authenticated or otherwise rejected.
Step 6. 2: if the sensor node is authenticated gateway node calculate $B = h(VID_i||p||T_4)$. $E= h(h(SP_i)||t||T_5)⊕B$ and both E and T5 to sensor node. After receiving message from G, V verifies the validity, calculate B= E ⊕h(h(SPi)||t||T5) and store this values in a safe place.

ii. Login Stage

If the user U_i is interested access data from sensor node V, he must insert his smart card into smart card system and enter user Id, password, and r value. Then the entered values used to calculate the following values:
Step 1: calculate new $h(r \| Pi) = UPN_i$ get T_1 $h(IDi)⊕T_1$, and T_2 from $h(T_1)⊕T_2$
Step 2: calculate B= C⊕h(y||T_2||ETi)
Step 3: calculate IDi = IDi*⊕h(ETi||T_3||T_4||B)
Step 4: calculate new P_i* = h(T3||T4||ETi || UPN_i)
Step 5: calculated ID, password is compared with received ID, password is matched then user is allowed to access or otherwise rejected.
Step 6: calculate NID = ID_i*⊕T_3⊕r
Step 7: calculate NID*= IDi⊕h(ETi||T_3||NID)
Step 8: calculate F = h(IDi||ETi ||B||T_4)
Step 9: Smart card sends (NID, NID*, F) to gateway node G

iii. Authentication Stage

After receiving a request from user Ui gateway node G complete the following works:
Step 1: Gateway node maintains the details ID_i*⊕r⊕h(p) of all users. G calculate NID⊕ ID_i*⊕r⊕h(p) to get h(p) ⊕ T_3. Finally G get the value of T_3.
Step 2: Checks the value of T_4-T_3> Δt and if it is true reject user request or otherwise proceed next step.
Step 3: Get T_1 from T_1⊕h(p||u) and gateway node G knows the value of p, u, ETi, T2 and IDi.
Step 4: calculate B= h(IDi||p||ETi), F*=h(IDi||ETi||B||T3), verifies that both F and F* is equal or not and if it is equal user is authenticated or otherwise rejected.

IV. Results and Discussions

i. Protecting from user impersonation attack

To perform user impersonation attack attacker must intercept the information which is exchanged between user U_i, gateway node G, and Sensor node. Attacker must access the stolen smart card of legitimate user and must calculate NID, NID*, F

to send login request to G. To prepare NID, NID*, F attacker must know the value of T_4, r, B, ID_i but attacker know the values of ET_i, C of user U_i. Therefore attacker is not in a position to prepare login request message and in our scheme it is impossible to force user impersonation attack

ii. Protecting from server impersonation attack

To impersonate like server (G) attacker must prepare a message and send to sensor node for that attacker need to know the values of ID_i, T_1, T_2, T_3, T_4 but attacker know the values of ET_i, C of user U_i. Therefore attacker is not in a position to prepare request message and in our scheme it is impossible to force server impersonation attack

iii. Protecting from man in the middle attack

To perform user man in the middle attack attacker must intercept the information which is exchanged between user U_i, gateway node G, and Sensor node. Here the attacker must act as user to G and act as G to user U_i. To act like user U_i, attacker need the values of NID, NID*, F which is not possible to get as our above discussion. Therefore our proposed method secure from man in the middle attack.

iv. *Stolen smart card attack*

Attacker even stolen the smart card of legitimate valid user Ui and try to get the values stored inside of smart card but attacker is not found any kind of valuable information about user Ui and G, that to Pi of user Ui to intercept or impersonate. So, our method is away from stolen smart card attack.

v. User anonymity

The attacker to intercept legitimate user IDi, he must calculate $IDi^* = IDi \oplus h(ETi||T_1||T_2||B)$, $IDi^* \oplus r \oplus h(p)$, $NID = IDi^* \oplus T_4 \oplus r$, $NID^* = IDi \oplus h(ETi||T4||NID)$. To know the value of IDi attacker must get the values of r, T_4, h(p), T_1, T_2, T_4. It is practically not possible to guess all these values and therefore our scheme is designed to protect user anonymity.

vi. Password protection

Attacker even stolen the smart card of legitimate valid user Ui and try to get the values stored inside of smart card but to calculate password $Pi= h(T_1||T_2||ETi||UPi)$ attacker must know the value of r, T_1 and T_2. In our proposed method is protecting from password guessing attack.

vii. Protecting from replay attack

In our proposed method all most all message which are transferred between user and gateway node or gateway node and sensor node contain time stamped values. Validity of each message is verified carefully so our scheme is free from replay attack.

V. Conclusion

A communication between user and sensor node may be authenticated but the attack may get the confidential values at gateway node. In the earlier method users are not verified at gateway node therefore attacker may be forcing attacks who resides like man in the middle between user and sensor node. In this paper we proposed a new method of mutual authentication method using temporal credential values. In our method user or sensor nodes both are verified at gateway node at different timings and if both are authorized then only gateway node allowed to communicate with each other. We have done cryptanalysis on earlier methods and we come to know that still there is a possibility of forcing attacks. At the end we discussed how our method provides solution for different attacks.

V. References

[1] Wong. K, Zheng. Y, Cao. J, Wang. S, "A Dynamic User Authentication Scheme for Wireless Sensor Networks", Proceedings IEEE International Conference on Sensor Networking, Ubiquitous, and Trustworthy Computing, PP 244-251, June 2006.

[2] Das. M. L, "Two-Factor User Authentication in Wireless Sensor Networks", IEEE Transaction on Wireless Communication, volume 8, Issue 3, PP 1086-1090, March 2009.

[3] Chen. T, Shih. W. K, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks", ETRI Journal, volume 32, number 5, PP 704-712, October 2010.

[4] Khan. M. K, Alghathbar. K, "Cryptanalysis and Security Improvements of Two-Factor User Authentication in Wireless Sensor Networks", Volume 10, PP 2450-2459, Sensors open access, March 2010.

[5] Yeh. H. L, Chen. T, Liu. P. C, Wei. H. W, "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors (14248220), Volume 11, Issue 5, PP 4767-4779, May 2011.

[6] Xue. K, Ma. C, Hong. P, Ding. R, "A temporal credential based mutual authentication and key agreement scheme for wireless sensor networks, Journal of Network and Computer Applications, Volume 36, Issue 1, PP 316-323, January 2013.

[7] Watro. R, Lynn. C, Kruus. P, Tiny. P. K, "Securing Sensor Networks with Public Key Technology", Proceedings of ACM Workshop Security Ad Hoc Sensor Networks, PP 59-64, 2004.