ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A NEW MUTUAL AUTHENTICATION AND IMPROVED SECURITY ANALYSIS OF XUE.K ET AL. APPROACH OVER WIRELESS SENSOR NETWORKS

M.Giri*[1], S.Jyothi[2]
[1]Research Scholar, PP Comp. Sci & Eng 0485, Department of CSE, Rayalaseema University, Kurnol, Andhra Pradesh, India.
[2]Professor, Department of Computer Science, SPMVV University, Tirupati, Andhra Pradesh, India.
Email: prof.m.giri@gmail.com

Received on: 25-02-2017 *Accepted on: 28-03-2017*

Abstract:

Day to day advancement in wireless communication technologies, in most of the application we are using sensors to collect more sensible data, but wireless sensor networks are insecure communication networks, and to protect gathered data from unauthorized users is challenging task in wireless sensor networks. But WSN demands high security features like authentication, key management techniques, and confidentiality. We propose a new more secure authentication approach to provide secure communication between either from user to gateway node or gateway node to sensor node. We done security analysis our existing and proposed approaches, our method protect against user impersonation, server impersonation, anonymity, password hacking man in the middle attack, stealing smart card, authentication, parallel session key and replay attack. After complete security analysis our proposed method out performing when compared with existing approaches.

Keywords: Session Key Management; Security Attacks; Impersonation; Authentication; Sensor Networks; Wireless Communication.

I. Introduction

The usage of wireless devices is rapidly increased due to technological development. More number of sensors is deployed in different remote locations to form sensor networks and then gather more useful information from deployed locations. In the same way advanced technology is used in web technologies to creating and retrieving information from various sources. Wireless communication technologies are embedded with web technology to share information from external sources through WWW and gives security issues in the communication. Sensors share information from source to destination via intermediate nodes over a network, it provides a chance to attacker to access more useful sensed data in an unauthorized way.To inherent Wireless sensor network with web technologies in

secured manner, we have to consider many security challenges and provide security to sensed data. We are planning to use mutual authentication approach to check user authenticity before sharing sensed data to users over wireless sensor networks. Many of the researchers worked on authentication mechanisms [1,2,3] with smart cards [5,6,7,8,9,10,11] to check user authenticity but nobody addressed all security attacks. The researcher [1] introduced a mechanism based on hash function, but researchers [2] done security analysis on [1] and they have provide that [1] is not protecting data from masquerade and counterfeit attacks. The researchers [3, 6, 10] done security analysis over [2] and they provide that [2] is not protecting data from replay attack. Using Elliptical curve cryptography [10] described authentication approach to share data from one sensor to target. The researcher Xue.K et al. presented timely based authentication approach to wireless sensor networks and described that all approaches [1, 2, 3, 6, 10] are not protect data from some of the attacks. In this research paper we proposed anew mutual authentication and improved security analysis of Xue.K et al. approach over wireless sensor networks. Intermediate node or gateway node issue timestamp to both user as well as sensors after checking identity and once timestamp reaches its lifetime then intermediate node update the time stamped values of authorized user.

II. Proposed Security Method

We propose a new novel authentication approach for secure exchange of keys in wireless sensor networks. It consists of three sub methods and users of wireless sensor networks are carefully verified at each stage in our proposed method. Some of the mathematical notations used in our proposed method are given below:

Ui = ith user of WSN; IDi =identification of ith user; SIDj= identification of jth sensor; Pi = password of ith user
NG= Gate Way Node; ki, kj=clandestine assessment value given by NG to user Ui and sensor Sj.
TS_{ei} = Expiry time of timeliness value TS_{cu} of Ui; a, b = random values selected by user Ui and sensor Sj
TS_{cs} =timeliness value of sensorSj.
H(.) = secure hash function; $\oplus$ = Bit by bit XOR operation
|| = Concatenation function

Table 1: List of users and the values of variable they known for security analysis.

User Type	Parameters used by the users	An authorized user may know the following list of values	An unauthorized user may know the following list of values
1	Values known by authorized user from his smart card: H(.), KID_i, P_i, $H(ID_i)\oplus ST_1$, $H(ST_1)\oplus RT_1$, TS_{ei}. User is not communicated either with gateway node or with internal node.	ID_i, SID_j, a, P_i, ST_1, RT_1, TS_{ei}, P_i, TS_{cu}, KID_i, ST_2	k_i, X_s, TS_{cs}, k_j, RT_2, ST_3, SST_1, RT_3, b, RTR_1.

2	An authorized user may have rights to interact with insider two know the following values: Smart card values: H(.), KID_i, P_i, $H(ID_i)\oplus ST_1$, $h(ST_1)\oplus RT_1$, TS_{ei}, PTC_i. he may be performed the following equations to know the values: $KID_{i1} = KID_i\oplus ST_2\oplus y$. $KID_{i2} = ID_i\oplus H(TS_{ei}\|\|ST_2\|\|KID_{i1})$. $C_i= H(ID_i\|\|TS_{ei}\|\|TS_{cu}\|\|ST_2)$; $KID_{NG}=ID_i\oplus H(TS_{cs})\oplus ST_3$. $CID_{NG}=H(ID_i\|\|TS_{cs}\|\|ST_3\|\|SID_j)$. $PD_{NG}=ST_3\oplus H(SID_j\|\|TS_{cs})$. $TD_{NG}=(ST_1\|\|RT_1\|\|ST_2\|\|RT_2)\oplus H(ST_3\|\|TS_{cs}\|\|ID_i)$. $DC_j = H(TS_{cs})\oplus(RT_3\|\|RT_2\|\|ST_3)$. $CS_j= H(S.K\|\| TS_{cs}\|\|ST_2\|\|ST_3)$. $DT_{NGi}=H(TS_{cu}\|\|ID_i\|\|ST_1)\oplus(RT_2\|\|ST_3\|\|RT_3)$. $CS_i= H(S.K\|\| TS_{cu}\|\|ST_1\|\|ST_2)$. He also knows the values there with NG: $KID_i\oplus y\oplus H(k_i)$, $TS_{ei}\oplus H(X_s\|\|k_i)$, $ST_1\oplus H(x_i\|\|X_s)$, $RT_1\oplus H(k_i\oplus X_s)$.	ID_i, a, P_i, ST_1, RT_1, TS_{ei}, P_i, PTC_i, TS_{cu}, KID_i, ST_2.	k_i, X_s, TS_{cs}, k_j, RT_2, ST_3, RT_3, b, RTR_1, SST_1.
3	The attacker with stolen smart card of U_i, he gets rights to know the following values from insider. One is all values from the smart card and the second one is the values mentioned in Row 2.	After stolen smart card of user U_i, an opponent can the values of TS_{ei}, P_i, of user U_i.	RT_1, TS_{cu}, KID_i, ID_i, a, P_i, ST_1, TS_{cs}, k_j, RT_2, ST_2, SID_j..k_i, X_s, ST_3, SST_1, b, RTR_1, RT_3.

We proposed new novel secure wireless communication technique to secure transfer of information from sensor to sensor. The proposed technique provides security in three stages: new user registration stage, login stage, and authentication stage.

A. User and Sensor Registration with NG

In this phase we assume that registered users ID, hash of password is stored in NG maintained database. Registration has two sub phases one is for users and the other one is for sensor. During user registration the following sequence of steps are executed.

Step 1: User Ui calculate RPi= H(a||Pi) and user send request message {IDi,RPi,ST1} to NG using secret communication line.

Step 2: After receiving registration message at timestamp RT1, and gateway node NG verify RT1-ST1 value. If the RT1-ST1 value is high then simply NG discards request message or otherwise NG tries to verify user authenticity by retrieve H(Pi) from NG users database.

NG calculates RPi* = H(a|| H(Pi)) and verifies that both RPi* and RPi are same or not, if it is not in NG simply discards the message request or otherwise calculate the following equations:

Pi= H(ST1||RT1||TS_{ei}||RPi)

TCi=H(IDi||ki||TS_{ei})

PTCi=TS_{cu}⊕H(a||RT1||TS_{ei})

KIDi=IDi⊕H(TS_{ei}||ST1||RT1||TS_{cu})

Gateway node NG loads KID⊕iy⊕H(ki), TS_{ei}⊕H(Xs||ki), ST1⊕H(ki||Xs), RT1⊕H(ki⊕Xs) in the users database.

Step 3: Gateway node prepare smart card with {H(.), KIDi, Pi, h(IDi)⊕ST1, H(ST1)⊕RT1, TS_{ei}} and transfer to user site through secret communication line.

Step 4: once sensor node Sj is deployed in wireless sensor network with {SIDj, Pj}, after that sensor node register with its NG for further communication.

Step 5: sensor Sj select random number 'b' and calculate RS = s⊕H(P)j, RPj = H(b||h(Pj)) and registration request message {SIDj, RPj, RS, STS1}to NG.

Step 6: After receiving registration message at timestamp RTR1, and gateway node NG verify RTR1-STS1 value. If the RTR1-STS1 value is high then simply NG discards request message or otherwise NG tries to verify sensor authenticity by retrieve H(Pj) from NG users database.

Step 7: NG calculates RS⊕H(Pj) = b, RPj* = H(b||H(Pj)) and verifies that both RPj* and RPj are same or not, if it is not in NG simply discards the message request or otherwise NG authenticate Sensor Sj.

Step 8: if Sj is genuine then gateway node NG calculates TS_{cs} = H(SIDj|| kj ||RTR1), REGj = H(H(Pj)||b||STS2)⊕ TS_{cs} and send back message {REGj, STS2}to sensor Sj. After receiving message from NG and Sj verify validity time. If it is valid then Sj calculates TS_{cs}= REGj⊕H(H(Pj)||b||STS2) and loaded in its hardware component for further reference.

B. Login Stage

When the user Uiis trying to contact sensor Sj for data, he has to swipe smart card into terminal to enter IDi*, Pi*,'a' and then perform the following operations.

Step 1:calculateH(a||Pi)* = RPi*, recover ST1 from H(IDi)⊕ST1 and RT1 from H(ST1)⊕RT1, calculate TS_{cu} = H(a||RT1||TS_{ei}) and IDi = KIDi⊕H(TS_{ei}||ST1||RT1||TS_{cu}).

Step 2: with the help of calculated values smart card calculate Pi*= H(ST1||RT1||TS_{ei}||RPi*) and verifies both Pi*and Pi are equal or not.

If both Pi* and Pi not equal reject login request message or otherwise do the following operations.

Step 3: calculate KIDi1 = KIDi⊕ST2⊕a, KIDi2 = IDi⊕H(TS_{ei}||ST2||KIDi1), Ci= H(IDi||TS_{ei}||TS_{cu}||ST2) , and smart card submit login request message {DIDi1, DIDi2, Ci}to gateway node NG.

C. Authentication Phase

After reception of request message at timestamp RT2 from userUi, Gateway nodes NG do the following operations:

Step 1: Gateway node NG stores KID⊕ai⊕H(ki) for Ui in the database as index to retrieve in future. The gateway node NG, calculate KIDi1⊕KID ⊕ai⊕H(ki) to retrieve H(ki)⊕ST2for all KID⊕ai⊕H(ki).

Step 2: Calculate RT2-ST2 value, if the value is high then simply reject request message or otherwise do the following operations.

Step 3: Get ST1 from ST1⊕H(ki||Xs) and gateway node NG knows the values of ki, Xs,TS_{ei}, RT1,IDi from KIDi2⊕ H(TS_{ei}||ST2||KIDi1).

Step 4: Calculate TS_{cu}= H(IDi||ki||TS_{ei}), Ci*=H(IDi||TS_{ei}||TS_{cu}||ST2) and verifies calculated Ci* is equal to received Ci or not. If it is same user is authenticated by gateway node NGor otherwise reject request message.

Step 5: Calculate TS_{cs} = H(SIDj|| kj ||RTR1), DIDNG=ID ⊕ iH(TS_{cs}) ⊕ ST3, CIDNG=H(IDi||TS_{cs}||ST3||SIDj),PDNG=ST3⊕h(SIDj||TS_{cs}), TDNG=(ST1||RT1||ST2||RT2) ⊕H(ST3||TS_{cs}||IDi), NG→Sj: {KIDNG,CIDNG, PDNG, TDNG} at timestampST3 to Sj.

Step 6: After receiving message from gateway node NG at timestamp, sensor node Sjdo the following operations.

Step 7: Get ST3 from PDNG⊕H(SIDj ||TS_{cs}) and verify RT3 - ST3, if the value is high then simply reject or otherwise do the following tasks.

Step 8: Get IDi fromKIDNG⊕ST3⊕H(TS_{cs}) = IDi, calculate CIDNG*= H(IDi||TS_{cs}||ST3||SIDj) and verifies CIDNG*is equal to received CIDNG or not.

If it is not equal reject or otherwise proceeds further. Retrieve (ST1||RT1||ST2||RT2), TDNG⊕H(ST3||TS_{cs}||IDi) = (ST1||RT1||ST2||RT2). The sensor Sjseparates the above equation toretrieve values of ST1, RT1, ST2, and RT2. .

Step 9: Calculation of session key, Key = H(IDi||ST1||RT1||ST2||RT2||ST3||RT3||TS_{ei}||SIDj), calculates DCj = H(TS_{cs})⊕ (RT3||RT2||ST3) and CSj= H(Key||TCj||ST2||ST3).

Step 10: Sensor send message {DCj, CSj} to gateway node NG. Receipt message from Sj, NG calculates DCj⊕ H(TS_{cs}) = (RT3||RT2||ST3) to retrieveRT3, RT2, ST3 and to calculate Key = H(IDi||ST1||RT1||ST2||RT2||ST3||RT3||TS_{ei}||SIDj).

Step 11: Calculates CSj*= H(S.K*|| TCj||ST2||ST3),verifiesCSj*with CSj, if it is same Sjis authenticated by gateway node NGor otherwise reject.

Step 12: Calculate DTNGi= H(TS_{cu}||IDi||ST1)⊕(RT2||ST3|| RT3), CSi= H(S.K|| TS_{cu}||ST1||ST2) and gateway node sends message { DTNGi, CSi } to user Ui.

Step 13: Calculate DTNGS⊕H(TS_{cu}||IDi||ST1) = (RT2||ST3||RT3) to retrieveRT3, RT2, ST3, frame key =H(IDi||ST1 ||RT1 ||ST2||RT2 ||ST3 ||RT3 ||TS_{ei}||SIDj), Calculate CSi * = H(S.K||TS_{cu}||ST1||ST2), verify CSi*with CSi. If it is same is user authenticates NGor otherwise simply reject.

If the key is calculated then all kinds of data exchange between Ui,gateway node NG, and sensorSj is encrypted with same key.

III. Security and Cost Analysis

In this section we did security analysis on proposed method with existing methods.

A. Protecting from replay attack

All kinds of messages transmitted between the Ui, NG, Sj has timestamp values which will helpful to detect replay attacks. In general messages are transmitting from user to gateway node, sensor to gateway node, and from sensor to user via gateway node. If the message is received by gateway node from user or sensor, first NG will check message generation time and reception time, if the time interval is small then NG will do further calculations or otherwise reject message. Therefore our proposed method is protecting from replay attack.

B. Protecting from gateway node bypass Attack

To calculate session key Ui must send RT2||ST3||RT3 to gateway node NG. Sensor node will transmit data to user after receiving signal from NG. If the user or attacker requested data directly from sensor node, in our method sensor will not send data to user without involvement of gateway node and therefore our method is away from gateway node bypass attack.

C. Protecting from parallel session attack

An attacker can impersonate like Ui by sending login request message with KIDi1, KIDi2, Ci within time bound. With help of insider attacker may guess the values of TS_{ei}, Pi, PTCibut still he has to guess IDi, ST1, RT1, ST2,

RT2, ST3, RT3 and which is not possible to guess all these values within time bound. So our method is protecting data from parallel session attack.

D. Mutual Authentication

In our proposed scheme, before starting communication both user and sensor must be authenticated by NG. After verification of both user and sensor gateway node generate session key and which is shared by both sensor and user for data exchange. Attacker may know the value of CSjwith that he may be guess IDi, ST1, RT1, ST2, RT2, ST3, RT3, TS_{ei}, TS_{cu}, $TS_{cs}$to frame key. It is not possible to guess all the above values. So our proposed method provides strong mutual authentication.

We did security analysis of proposed method with existing methods. In addition to above mention attacks it is possible to force some other types of attacks and we listed various types of attacks possible in table 2.

In this section, we are estimate communication cost of sensor node by applying SHA-1 algorithm and elliptical curve cryptography. In both proposed and Xue et al. [11] method we used 128 bit ID, 24 bit timestamp values, and generate 128 bit has code. Communication cost of sensor node in various methods is shown in table 3. Efficiency of the methods is calculated in terms of TH & TECC and it is shown in table 4.

Table 3: Communication cost of sensor nodes.

	Proposed	[3]	[6].	[7]	[9]	[11]
Sj.(bytes)	32	16	19	51	35	51

Table 4: Efficiency of various methods in terms of TH & TECC.

	Proposed	[2]	[3]	[6]	[10]	[11]
Ui	8TH+3 TH	3 TH	4 TH	3 TH	TH+2TECC	6TH+3 TH
Sj	5TH+1TH	TH	2 TH	2 TH	3TH+2TECC	5TH+1TH
NG	10TH+4 TH	4TH	5 TH	5 TH	4TH+4TECC	10TH+3 TH

Table 2: Security analysis of proposed method over existing method.

Security attack	Proposed	[1]	[2]	[3]	[5]	[6]	[10]	[11]
Protecting from replay attack	√	X	√	√	√	√	X	X

Protecting from server impersonation attack	√	√	X	X	X	√	√	X
Protecting from parallel session attack	√	X	X	X	√	√	X	X
Mutual authentication	√	X	X	√	X	√	√	X
Protecting from user impersonation attack	√	√	X	X	X	√	√	X
Protecting from Gateway node bypass attack	√	X	X	X	X	X	X	X
Protecting from Man in the middle attack	√	√	X	X	X	√	√	X

IV. Conclusion

In this paper, we have proposed A New Mutual authentication and improved security analysis of Xue.K et al. Approach over Wireless Sensor Networks. It consist of three phases: Login phase, registration phase, and authentication phase. Before transmitting data both user and sensor must be register with gateway node. All kinds of data transmission from sensor to user past through gateway node. To provide authentication we have used SHA-1 algorithm and Elliptic curve cryptography. We did security and cost analysis of our method with other existing methods. From our analysis we come to know that our method is protecting data from various types of security attacks when compared with other methods.

V. References

1. Wong.K, Zheng.Y, “A Dynamic User Authentication Scheme for Wireless Sensor Networks,”, Proceeding IEEE International Conference on Sensor Networks, Ubiquitous, Trustworthy Computing, Pages 244-251, 2006.
2. Das.M..L, “Two-Factor User Authentication in Wireless Sensor Networks,” IEEE Transactions on Wireless Communications, volume 8, number 3, pages 1086-1090, 2009.
3. Chen.T, Shih.W, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks," ERTI Journal, volume 32, number 5, pages 704-712, October 2010.

4. Diffie.W , Hellman.M, "New directions in cryptography", IEEE Transactions on Information Theory, volume 22, Issue 6, pages 644-654, November 1976.
5. He.D, Gao.Y, Chan.S, "An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks", Ad-hoc and Sensor Wireless networks, Volume 0, pages 1–114, 2010
6. Khan.M.K, Alghathbar.K, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'". Volume 10, pages 2450-2459, Sensors, 2010.
7. Song.R, "Advanced smart card based password authentication protocol", Computer Standards & Interfaces, Volume 32, Issue 4, , Pages 321-325, June 2010
8. Wang.Y, Wong. K, "A Dynamic User Authentication Scheme for Wireless Sensor Networks". SUTC'06, pages 32-58, June 05-07, 2007.
9. Xu.J, Feng.W, "An improved smart card based password authentication scheme with provable security", Computer Standards & Interfaces; Volume 31, Issue 4, Pages 723–728, June 2009.
10. Yeh.H.L, Chen. T, "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors, Volume 11, Issue 5, pages 4767-4779, 2011.
11. 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, Pages 316-323, January 2013.