

# Secure data exchange from one sensor node to other sensor node through arbitrary node over wireless sensor networks

M.GIRI\*, Dr.S.JYOTHI\*\*

\*Research Scholar, Department of CSE, Rayalaseema University, Kurnol, India, prof.m.giri@gmail.com

\*\*Professor, Department of Computer Science, SPMVV University, Tirupati, Andhra Pradesh, India, jyothi.spmvv@gmail.com

**Abstract**—In the modern world many of the wireless devices are used to geographical gather information. Attacker is residing on network or gateway node. Data which is transmitted from user to sensor or sensor to user is continuously monitored by the attacker to capture valuable data. With that attacker is going to force attacks in an unauthorized way. In this paper, we propose a new novel secure mutual authentication approach. In this method we used temporal values to protect data. In our approach both user and sensor nodes separately register with its gateway sensor node, gateway node issue smart card to user and sensor node. We applied cryptanalysis on the existing method but it is possible to force some of the attacks. After cryptanalysis, our method protecting data from all possible security attacks when compared with existing method.

**Index Terms**—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 [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, 10] 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, 9] proposed elliptical curve cryptography based mutual authentication to solve the weakness there 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 [1].

### III. PROPOSED METHOD

List of notations used in the proposed system.

$U_i \rightarrow$  ith user  
 $ID_i \rightarrow$  user  $U_i$  ID.  
 $SID_j \rightarrow$  Sensor node ID.  
 $P_i \rightarrow$  the password of user  $U_i$ .  
 $G \rightarrow$  Gateway node  
 $p, q \rightarrow$  Gateway node assigns secret values to user  $U_i$  and server  $V$   
 $ET_i \rightarrow$  Temporary credentials of user  $U_i$   
 $r \rightarrow$  random value selected by user  $U_i$   
 $t \rightarrow$  random value selected by sensor node  $V$   
 $u \rightarrow$  temporal value for sensor node  $V$   
 $h(.) \rightarrow$  hash function  
 $\oplus \rightarrow$  Bitwise exclusive OR function  
 $\parallel \rightarrow$  Concatenation

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

#### A. 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  $UP_i = H(r \parallel P_i)$  and at time stamp  $T_{1user}$   $U_i$  send request message ( $ID_i, UP_i, T_1$ ) to gateway node  $G$  through secure way.

Step 2: after receiving request from user  $U_i$  at time  $T_2$  then  $G$  verifies that is it  $T_2 - T_1 > \Delta t$ , if it is the case then  $G$  simply reject user request or otherwise user is verified by getting  $h(P_i)$  from gateway node database using  $ID_i$  and then calculate new password  $UP_{Ni} = h(r \parallel h(P_i))$  and verifies if both password is same then user is allowed to proceed further by calculating following calculations or otherwise user is rejected.

$$A = H(T_1 \parallel T_2 \parallel ET_i \parallel UP_i)$$

$$B = H(ID_i \parallel p \parallel ET_i)$$

$$C = B \oplus H(r \parallel T_2 \parallel ET_i)$$

$$ID_i^* = ID_i \oplus h(ET_i \parallel T_1 \parallel T_2 \parallel B)$$

The gateway node  $G$  stores values  $ET_i \oplus H(u \parallel p)$ ,  $ID_i^* \oplus r \oplus H(p)$ ,  $T_2 \oplus H(p \oplus u)$ ,  $T_1 \oplus H(p \parallel u)$  into database.

Step 3: By using secret channel gateway node  $G$  issued smart card to user which contain values ( $ID_i^*$ ,  $H(ID_i) \oplus T_1, ET_i, C, H(T_1) \oplus T_2$ ).

Step 4: Each sensor node  $V_i$  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  $V_i$  selects a random number  $t$ , calculate  $D = t \oplus H(SP_i)$ ,  $UP_i = H(t \parallel H(SP_i))$  and send request to gateway node  $G$  ( $VID_i, UP_i, D, T_3$ ).

Step 6: After receiving sensor node registration request at  $T_4$ , gateway node verifies that  $T_4 - T_3 > \Delta t$  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  $H(SP_i)$  from database by indexing its identity, calculate  $D \oplus H(SP_i) = t$ ,  $UP_{Ni} = H(t \parallel H(SP_i))$ , verifies that  $UP_{Ni}$  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  $B = H(VID_i \parallel p \parallel T_4)$ .  $E = H(H(SP_i) \parallel t \parallel T_5) \oplus B$  and both  $E$  and  $T_5$  to sensor node. After receiving message from  $G$ ,  $V$  verifies the validity, calculate  $B = E \oplus H(H(SP_i) \parallel t \parallel T_5)$  and store this values in a safe place.

#### B. 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  $ID_i$ , password, and  $r$  value. Then the entered values used to calculate the following values:

Step 1: calculate new  $H(r || P_i) = UPN_i$  get  $T_1$  from  $H(ID_i) \oplus T_1$ , and  $T_2$  from  $H(T_1) \oplus T_2$

Step 2: calculate  $B = C \oplus H(y || T_2 || ET_i)$

Step 3: calculate  $ID_i^* = ID_i \oplus H(ET_i || T_3 || T_4 || B)$

Step 4: calculate new  $P_i^* = H(T_3 || T_4 || ET_i || UPN_i)$

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  $NID = ID_i^* \oplus T_3 \oplus r$

Step 7: calculate  $NID^* = ID_i \oplus H(ET_i || T_3 || NID)$

Step 8: calculate  $F = H(ID_i || ET_i || B || T_4)$

Step 9: Smart card sends ( $NID$ ,  $NID^*$ ,  $F$ ) to gateway node  $G$

#### C. Authentication Stage

After receiving a request from user  $U_i$  gateway node  $G$  complete the following works:

Step 1: Gateway node maintains the details  $ID_i^* \oplus r \oplus H(p)$  of all users.  $G$  calculate  $NID \oplus ID_i^* \oplus r \oplus H(p)$  to get  $H(p) \oplus T_3$ . Finally  $G$  get the value of  $T_3$ .

Step 2: Checks the value of  $T_4 - T_3 > \Delta t$  and if it is true reject user request or otherwise proceed next step.

Step 3: Get  $T_1$  from  $T_1 \oplus h(p || u)$  and gateway node  $G$  knows the value of  $p$ ,  $u$ ,  $ET_i$ ,  $T_2$  and  $ID_i$ .

Step 4: calculate  $B = H(ID_i || p || ET_i)$ ,  $F^* = H(ID_i || ET_i || B || T_3)$ , verifies that both  $F$  and  $F^*$  is equal or not and if it is equal user is authenticated or otherwise rejected.

### IV. SECURITY ANALYSIS AND DISCUSSIONS

#### A. 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.

#### B. 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

#### C. 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.

#### D. Stolen smart card attack

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

#### E. User anonymity

The attacker to intercept legitimate user  $ID_i$ , he must calculate  $ID_i^* = ID_i \oplus h(ET_i || T_1 || T_2 || B)$ ,  $ID_i^* \oplus r \oplus h(p)$ ,  $NID = ID_i^* \oplus T_4 \oplus r$ ,  $NID^* = ID_i \oplus h(ET_i || T_4 || NID)$ . To know the value of  $ID_i$  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.

#### F. Password protection

Attacker even stolen the smart card of legitimate valid user  $U_i$  and try to get the values stored inside of smart card but to calculate password  $P_i = h(T_1 || T_2 || ET_i || U_P_i)$  attacker must know the value of  $r$ ,  $T_1$  and  $T_2$ . In our

proposed method is protecting from password guessing attack.

#### G. 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.

#### 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.
- [8] Xu.H, Hua.K, "Secured ECG Signal Transmission for human emotional stress classification in wireless body area networks", EURASIP Journal of Information Security, Springer, January, 2016.
- [9] XuXun Liu, "A typical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review", IEEE Sensor Journal, Volume 15, Issue 10, PP 5372-5383, October 2015.
- [10] Fagen Li, "Efficient Certificate less Access Control for wireless body area Networks", IEEE Sensor Journal, Volume 16, Issue 13, Pages 5389-5396, April 2016.
- [11] James Brusey, "Energy Profiling in Practical Sensor Networks: identifying Hidden Consumers", IEEE Sensor Journal, Volume 16, Issue 15, Pages 6072-6080, August 2016.