International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Highly Secure and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks

Apurva J. Shastri[1], S. R. Tandle[2]

[1]PG Student, Department of CSE, M. S. Bidve College of engineering, Latur, Maharashtra, India

[2]Assistant Professor and Head of CSE Department in M. S. Bidve College of engineering, Latur, Maharashtra, India

Abstract: ***In Wireless Sensor Network, when user wants to access the data at sensor node at that time user should be authorized. There are many malicious users in network. In previous systems, there are chances of many network attacks like node capture, stolen smart card attack, sensor node spoofing attack, stolen verifier attack, and fails to ensure backward secrecy. To overcome these attacks and to prevent our sensor, sensor data, and Network from malicious users, we proposed a secure, efficient, flexible Authentication Scheme for WSN.***

Keywords: Ad hoc wireless sensor network, Smart card, Forward Secrecy, Oracles

1. Introduction

A Wireless Sensor Network consist of voluminous number of specialized and autonomous sensors exchanging data with each other over wireless network.

They are mainly used in real-time monitoring applications like monitoring of traffic, monitoring of environmental conditions, monitoring of wildlife, security of homelands and controlling battlefield weapons. So they may contain confidential or important information that should be accessed by legitimate user. If the user wants to instruct the sensor node to perform certain task then he must be authenticated before sending instructions to the sensor nodes.

The authentication in wireless sensor networks is done in two ways:

- A user is authenticated by gateway node before communicating Sensor node.
- A user can directly communicate with sensor node for its authentication.

A sensor node is having some limitations such as-low memory, low battery power, low bandwidth, and limited computation ability. Due to limitations of wireless sensor networks lightweight authentication and key agreement protocols are chosen for wireless sensor networks.

2. Terminologies USED

The following table depicts the terminologies used in this paper.

Table 1: Terminologies Used

U_i	The user
ID_i	The identity of U_i
PW_i	The password of U_i
SC_i	The smart card of U_i
GWN	The gateway node
S_j	The sensor node
SID_j	The identity of S_j
X_{GWN}	The long-term secret of GWN
X_{GWN-U_i}	The secret shared between GWN and U_i
X_{GWN-S_j}	The secret shared between GWN and S_j
T_1, T_2, T_3, T_4	The timestamps
ΔT	The expected transmission delay
$r_i, r_i', r_j, K_i, K_j, a, b$	The random numbers
P	A point on the elliptic curve
$P.x$	The x-axis value of the point P
$\|\|, \oplus, h()$	The concatenation, XOR, and hash operation

2.1 Interaction in sensor networks

When a user Ui wants to interact securely with a sensor node Sj in a Wireless Sensor Network then procedure is as follows:

1) Ui first sends a login message (1) directly Sj which subsequently requests (2) the gateway node GWN for authenticating the user.
2) When receiving positive response (3) from GWN, the sensor node accepts Ui and replies with key establishment information (4).

2.2 Instances or Oracles

Let the instance t of the sensor node Sj be π_{Sj}^{t} the instance u of the user IDi be π_{Ui}^{u} and the instance v of the gateway node GWN be π_{GWN}^{v} these instances are called oracles.

1.3 Adversary

The adversary A is assumed to have complete control over all the communications in aWSN. Besides the ability to read and modify all the exchanged messages, A can also create new messages and enforce them into the network. Adversary is able to perform active as well as passive attacks.

3. Literature Survey

In 2006, wong et. Al.[2] proposed strong password based dynamic user authentication scheme which imposes very light computational load and works on single operations like one-way hash function and exclusive-or operations. They made use of security features on MAC sublayer (medium access control) based on IEEE 802.15.4 specification.

In 2007, Tseng et. Al. [3] have proposed scheme which showed that Wong et. Al. scheme was vulnerable to replay and forgery attacks. They proposed scheme which possesses

Many pros such as resistance of replay and forgery attacks .It also reduced the leackage threat of users password as well as managed to change password freely with better efficiency. But the limitation of this paper was achieving mutual authentication between users and sensor nodes as well as with centralized GWN.

In 2009, M. L. DAS presented a two factor user authentication scheme for WSN, which was mainly intended to obtain strong authentication, session key establishment, and efficiency of the system. The basic idea was user will receive smart card during its registeration phase and he can be authenticated with the help of this smart card and his password. But the limitation of this system was experimental results were needed to display feasibility of this scheme and also the counteracts against the denial-of-service and node compromise attacks were not provided.

In 2010, [8] proposed an improved two-factor scheme which showed that Das scheme have flaws are vulnerable to attacks like stolen smart card attack and which was resistant to stolen smart card attack as well as other common type of attacks. They depicted security evaluation and and efficiency analysis which showed that proposed scheme was more robust and secure than existing system.But the limitations of these scheme was it didn't provided session key agrrement and mutual authentication between user and sensor node/GWN. Also the computational overhead of propoed system was insignificantly higher than aforementioned schemes.

In 2014, Turkanovic et. Al. proposed a lightweight authentication and key agreement scheme for heterogeneous Ad hoc wireless sensor networks where user can exchange session key with sensor node to which it wants to access very securely by using simple hash and XOR computations. The main aim of paper was providing access of sensor node to remote user without directly contacting the Gateway Node. But the limitation of this paper was the scheme he proposed was prone to attacks like stolen smart card attack, impersonation attack with node capture, sensor node spoofing attack, stolen verifier attack and this scheme was also unsuccessful in providing backward serecy.

4. Proposed System

Our proposed system basically provides perfect forward secrecy as compared with previous existing system. In this paper we basically develop secure, efficient, flexible authentication scheme for adhoc wireless sensor network using smart card approach. In this approach, we propose a system to authenticate user using Elliptic Curve Cryptography (ECC) using smart card. Here smart card used for identity of user. This approach works in two modes. The first mode provides a lightweight authentication scheme which overcomes the weaknesses in Turkanovic et al.'s but this mode does not provide perfect forward secrecy. Advantage of this scheme is it does not require database storage at gateway nodes for the shared secrets.

The second mode is an advanced protocol based on ECC which provides perfect forward secrecy. Depending on application and the security level required, the user can choose which mode to be used.

The proposed scheme is mainly divided into four phases which are pre-deployment phase, registration phase, authentication phase, and password changing phase.

Pre-deployment Phase
In this phase GWN is provided a randomely generated long term secret XGWN . Before deploying into network all the m sensor nodes in the network where $1 \leq j \leq m$ has provided with identity SIDj .

Registration phase
Every user Ui who want to access sensor node sj from given WSN first has to be registered on the network. User has to provide IDi and password PWi. Where GWN verifies the users identity and personalizes smart card SCi for that particular user which is assigned to the user after completion of this phase.

Authentication Phase
In this phase when the user Ui want to communicate with sensor node in the deployed network he has to login to the system where he has to provide his id IDi and password PWi. After login phase user Ui will be verified by sensor node, GWN, smart card SCi in different steps with algorithmic computations and if user details are correct then he has given access to Sj else session is terminated.

Password Changing Phase
The authenticated user of the system can use this facility of the system. Where he has to provide his id IDi and password PWi along with his smart card details. User Ui has requested to enter the new password PWi^{new}. Now smart card computes new calculations and the password will be changed.

5. Conclusion

The earlier studies on this topic have gone through many issues like replay attacks, forgery attacks, leakage threat of password. The most recent scheme proposed by Turkanovic et. al's. also suffers from stolen smart card attack where the intruder lags into sensor node. Second, It undergoes node spoofing attack .Adversary can also obtain past and future session keys. This scheme also suffers from stolen verifier attack where adversary pretends as sensor node. Our proposed scheme overcomes from all these attacks. The first

protocol p1 can be used in lightweight environment and the second protocol p2 can be used in extreme hostile environment and it also provides forward secrecy.

References

[1] M. Turkanovic, B Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Netw., vol. 20, pp. 96–112, Sep. 2014.
[2] K. H. M.Wong, Y. Zheng, J. Cao, and S.Wang, "A dynamic user authentication scheme for wireless sensor networks," in Proc. IEEE Int. Conf. Sens. Netw. Ubiq. Trustworthy Comput., Jun. 2006, vol. 1, pp. 244–251.
[3] H. R. Tseng, R. H. Jan, andW. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in Proc. IEEE Global Telecommun. Conf., Nov. 2007, pp. 986–990.
[4] M. L. Das, "Two-factor user authentication in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 8, no. 3, pp. 1086–1090, Mar. 2009.
[5] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," Sensors, vol. 10, pp. 2450–2459, Mar. 2010.
[6] T. H. Chen and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks," ETRI J., vol. 32, no. 5, pp. 704–712, Oct. 2010.
[7] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," Ad Hoc Sens. Wireless Netw., vol. 10, no. 4, pp. 361–371, 2010.
[8] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in Proc. IEEE 6th Int. Conf. Wireless Mobile Comput. Netw. Commun., Oct. 2010, pp. 600–606.
[9] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," J. Netw. Comput. Appl., vol. 35, no. 5, pp. 1646–1656, Sep. 2012.
[10] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 316–323, Jan. 2013.
[11] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credential based security scheme with mutual authentication and key agreement for wireless sensor networks," Sensors, vol. 13, pp. 9589–9603, Jul. 2013.
[12] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," Electron. Elect. Eng., vol. 19, no. 6, pp. 109–116, 2013.

Author Profile

Apurva J. Shastri received the B.E. degree in Computer Science And Engineering from M. S. Bidve College Of Engineering, Latur, Maharashtra, India and now she is pursuing Master's of Engineering in Computer Science And Engineering from M. S. Bidve College Of Engineering, Latur, Maharashtra, India.

Prof. Shrikant R. Tandle has done B.E.(Electronics) from SGGS College of Engineering and Technology, Nanded and M.E.(Computer Science and Engineering) from MGM College of Engineering, Nanded. He is working as Assistant Professor and Head of CSE Department in M.S.Bidve Engineering College, Latur since 1990. He is pursuing his research work in Wireless Sensor Networks in Swami Ramanand Teerth Marathwada University, Nanded