|| Volume 3 || Issue 4 || April 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A Review on - Most Secured and Flexible Authentication Scheme for Adhoc Wireless Sensor Networks

Apurva J. Shastri[1], Vinayak D. Shastri[2]
PG Student, Department of CSE, M. S. Bidve College of engineering, Latur, Maharashtra, India.[1]
Assistant Professor and Training & Placement Officer in MPGI SOE, Nanded, Maharashtra, India.[2]

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, Cloud Storage*

I 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.

II RELATED WORK

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 sub layer (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 leakage 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.

III SYSTEM DEVELOPMENT

3.1 Existing System with Mathematical Model

User Registration:
First, we enter the user ID and Password (ID, PW) and one random number(r).
Using hash function concatenation random(r) and password(PW) and store MP variable.
MUreg is store User ID and MP. And send to Gateway node Gateway nodes choose randomnumber (r).
MI is store random number and user id concatenation using hash function.
Fi is store MI and long-term secret of gateway nodes concatenation using hash function.
Here used _ operator
The expression MP_ Fi is true if only one of MP _ Fi is true, it is false if both are true or ifboth are false.
Then Gateway nodes create smart card.
SC=MI, ei.
Then user create random number SCI=MI,ei,ri.
Authentication Phase: using P1 protocol
User Ui
(SC=MI,ei,ri)
Input enter ID and PW
SC compute MP=concatenation between random number and Password using hash function.
Fi =The expression ei_ MP is true if only one of ei _ MP is true, it is false if both are true
or if both are false. Get T1 means current event time.
Y=concatenation between Fi and Ti using hash function
Then select Random Number K
Z=The expression K_ Y is true if only one of K _ is true, it is false if both are true or ifboth are false.
N=concatenation between Y, MI and SID using hash function.
M=store the MI,Z,N,T1. Send to sensor node.
Sensor node
store Fi=concatenation between SID and secret of Gateway nodes using hash function
Check T1 Then get T2(Current event time)

A=concatenation F , N and T2 using hash function and store m2. m2=MI,N,SID,A,T1,T2
GWN (store XGWNSID,XGWN-SandMI,XGWN-U)
Check T1 and T2.
Compute
Fj=concatenation between SID and XGWN-U using hash function.
A=concatenation between F,N and T2 using hash function.
FI =concatenation between MI and XGWN using hash function.
Y=concatenation between Fi and T1 using hash function.
N=concatenation between Y,MI and XGWN-U using hash function.
Check N=N and A =A
Get current event time T3.
Compute.

IV CONCLUSION

The system shows that Turkanovic et al.'s scheme is vulnerable to various kinds of attacks. First, an adversary can log into a sensor node with a stolen smart card. Second, the adversary can impersonate a user to access to any sensor node or mount sensor node spoofing attack after compromising a sensor node. Moreover, the adversary can obtain the past and the future session keys.

REFERENCES

[1] M. Turkanovic, BBrumen, 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 authenticationscheme 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.Elect. Eng., vol. 19, no. 6, pp. 109–116, 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.