International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 3, Issue 12, December 2015.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

WIRELESS SENSOR NETWORKS: PATTERN OF AMBIGUITY PROTECTING THREE-FACTOR SUBSTANTIATES ACCESS FOR TRANSACTION CODE

A.Suresh Kumar[1], M.Kannan[2]
[1]Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.
[2]Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

Abstract: Many issues have been detected in the security process like guessing password attack in offline, user imposture attack, stolen smart-card attack, etc., in sensor networks. For enhancing the network security and specific application's security 3-Factor Substantiate Access (3-FSA) mechanism with pattern ambiguity protection is proposed. The pattern ambiguity generates the hashing key for protecting the data and controls the user by the way of gateway node. The transaction code is generally included with private identification number with session keys. In order to protect the network from data breaches and other risks posed by hackers a method called patented inaccessible installation was used along with the proposed three-factor substantiate mechanism.
Keywords: 3 Factor Security, Forward and Reverse keys, AVISPA, Transaction verification, WSN.

Introduction:

WSN is made out of numerous 3 minimal effort and low-control sensor gadgets. These sensor hubs are sent physically or arbitrarily finished any objective district. WSN has turned into a new and 6 well known innovation for its potential applications in ecological checking, horticulture, medicinal services, fiasco administration, and household with observation frameworks. The capacity of a sensor organize in general relies upon the utilitarian abilities of person individuals. A broken sensor may posture significant issues as far as precision and honesty of information on the off chance that it isn't been discovered what's more, tended to legitimately. This test turns out to be considerably more hard to overcome for huge scale sensor systems, where the impact of low confirmation can increase. [1]Unwavering quality, for instance, of detected information from a system is one imperative issue to be tended to. Furthermore, since (conceivably basic) basic leadership is made in view of the collected data gathered in the system, even little scale assaults or blames can have genuine consequences.

User favours low-entropy password in two-factor authentication protocols [3], which is selected from a small dictionary based on password and smartcard. The adversary performs the off-line procedure to guess user's password within polynomial time in the outcome. Therefore, two factor authentication systems cannot provide high security due to the off-line password guessing attack. Therefore 3 factor authentication mechanism is concentrated for providing highly confidential services.

Related Works:

Many user authentication and key agreement protocols have been proposed in the literatures to upgrade the functionalities and securities in WSNs. The security loopholes of the authentication protocols proposed is discussed here briefly. The User Authentication And Key Agreement (UAKA) protocol [2] is susceptible to gateway node bypassing attack and privileged insider attack. Most of the sensor networks suffer from the privileged insider attack and user impersonation attack, and they presented an extended two-factor user authentication protocol as a remedy. A user authentication protocol for two-tire WSN [4] was introduced to overcome the hacking and vulnerabilities produced by the conventional scheme. Biometric-based three-factor user authentication protocol for WSNs was proposed which was in-secure against forgery attack and is vulnerable to information leakage attack and it is unable to preserve user anonymity and mutual authentication property.

Two user authentication protocols was proposed [6] that provides registration and authentication of nodes, however due to malicious finders in build network it was proved to be imperfect, hence two enhanced protocols was proposed to deal with the security ambiguities of the protocol and then put forwarded. Further, the 2 - User Authentication [8] protocol provides a solution against sensor node capture attack. Hash function based light-weight user authentication protocol for heterogeneous ad-hoc WSNs using the concept of IoT was proposed.

Cryptanalysis and improvement of a user authentication scheme examined preserving uniqueness [5] and found that it cannot withstand user anonymity problem smartcard stolen attack, off-line password guessing attack, new smartcard issue attack, user impersonation attack and known session specific temporary information attack.

In addition, ECC key [7] is added for the light weight protocol contributes post deployment phase, identity change phase, password change phase and smartcard revocation phase

3. Proposed Method:

Three factor authentication protocols based on password, smartcard and biometric gain popular for producing secured individual identity factors for verification. In three-factor authentication protocol, user enjoys high security over two-factor protocol due to the biometric cannot be forgotten and biometric data cannot be guessed easily. In order to tackle the password guessing attack, a framework is proposed to upgrade two-factor authentication system to three-factor system which is shown in the figure 1.

Security three-factor substantiate mechanism with pattern ambiguity protection is proposed with user identity periodic update phase that functions non-invertible manner that can generate protected biometric template. Numerous authentication protocols have been utilized protected biometric template to identify the genuine user.

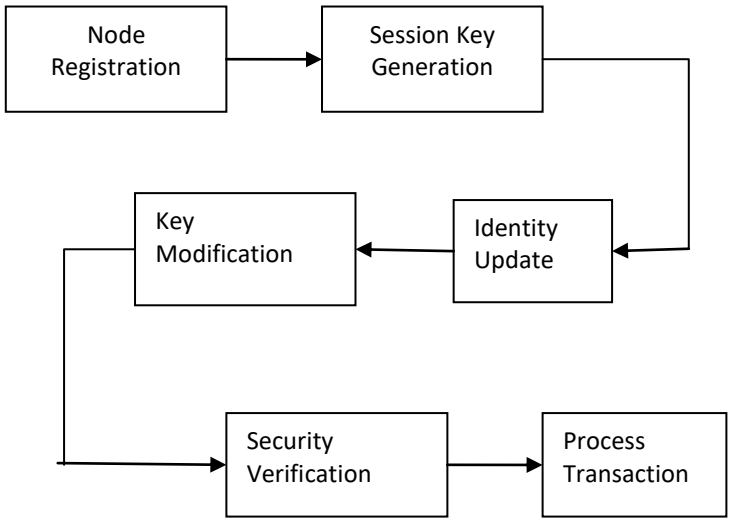

Figure.1. Framework of 3-FSA

Registration session key concurrence phase:

A function module is created and the nodes that are deployed are to be registered with the help of function module. The function module consists of System Administrator (SA) and allocates the module in to trust module, distrust module and uncertainty module. By generating a random number node privacy is calculated with the session key generated timestamp [T1, T2]. Based on the session timestamp the message secrecy rate is processed. If the message and individual identity number is entered within the timestamp T1, then the input key is generates the message as session valid, else T1 session gets abort and the identity phase gets updated.

Identity Revise phase:

The main intention of this phase is to update the identity of the registered user securely. This phase needs the assistance of gateway node to update the identity. Ui inserts the smartcard into the card reader and executes the login phase to verify Ui's legitimacy.

Key modify phase:

Due to security reason, an authorized user Ui wants to update the password PWi. Therefore, password-based authentication protocol must include password change facility. In order to reduce the complexity and network congestion, the password change must be done without any help of SA or GWN.

Security Verification phase:

AVISPA software tool is used generally to verify the security correctness and it is widely accepted for security measures. The authentication mechanism includes estimation of forward key F_{key} and reverses key R_{key} from source to destination node. If fault detected then the neighbour node is termed to be malicious and session key closed with transaction error. If F_{key} and R_{key} are equal and the process terminated successfully and if both the keys are not equal then it results with transaction error.

Algorithms – Security Verification

3-F auth ()
{
User S sends $L3_{REQ}$ to the node N
S estimates $F_{KEY} \leftarrow I+J$;
N replies with estimated $R_{KEY} \leftarrow J+K$;
If (R_{KEY} !=F_{KEY}){
Remove N from neighbour list
Broadcast N is 'malicious'
Generate Error message
Set false alarm high
Return 1
} end if
Else {
Process transaction request successfully
Return 0
} **end else**
} **end**

4. Results and Discussion

Three metrics are considered for the analysis of secured transaction process in sensor networks. They are Deliverance Rate, Transaction Delay, and Detection Rate.

Deliverance Rate

The Delivery Rate (PDR) of packets that are transmitted by the source is defined as the ratio of the total number of packets successfully delivered to the receiver. It is obtained from the equation (1) below.

$$PDR = \frac{\sum_{0}^{n} PktsDelivered}{Time} \quad (1)$$

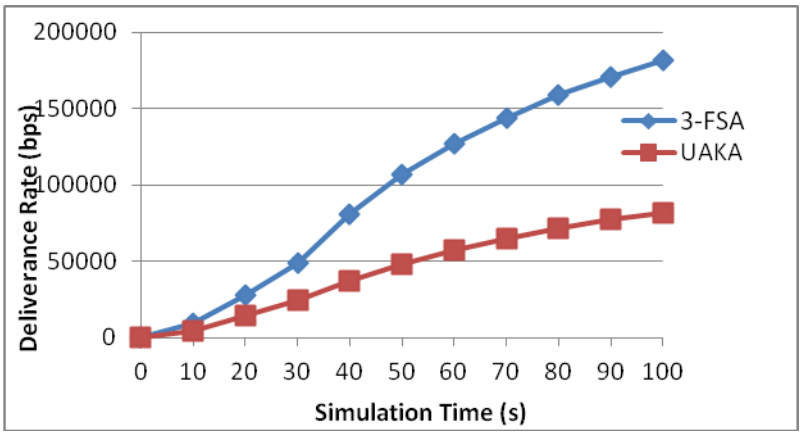

Figure 1. Deliverance rate

The figure 2 represents the obtained deliverance rate for both proposed and conventional scheme. Proposed scheme gives better output than the UAKA scheme.

Transaction Delay

Delay is defined as the time difference between the data entered for transaction and time taken for ending the transaction process including node verification, evaluate by the equation (2) below. The figure 3 describes the transaction delay for the proposed and existing protocol. 3-FSA has better output then the UAKA and saves the time in efficient manner.

$$Delay = \frac{\sum_{0}^{T2-T1} Transaction\ process\ time}{n} \qquad \{0 \leq PDR \leq T2 - T1\} \quad (2)$$

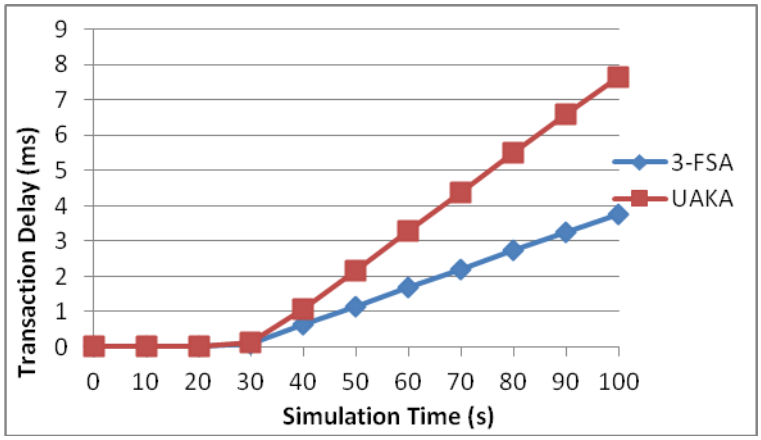

Figure 3. Transaction Delay

Detection Ratio

The false detection ratio is detecting the malicious nodes from the deployed nodes. False Detection Ratio is defined as follows in equation 3,

$$FDR = \frac{M_{pn}}{T_{nn}} \qquad \{0 \leq FDR \leq 1\} \quad (3)$$

M_{pn} is the no of normal nodes misidentified as the precarious node by one or more normal nodes and T_{nn} is the total no of normal node. Figure 3 shows the transaction delay for both 3FAS and existing UAKA protocol.

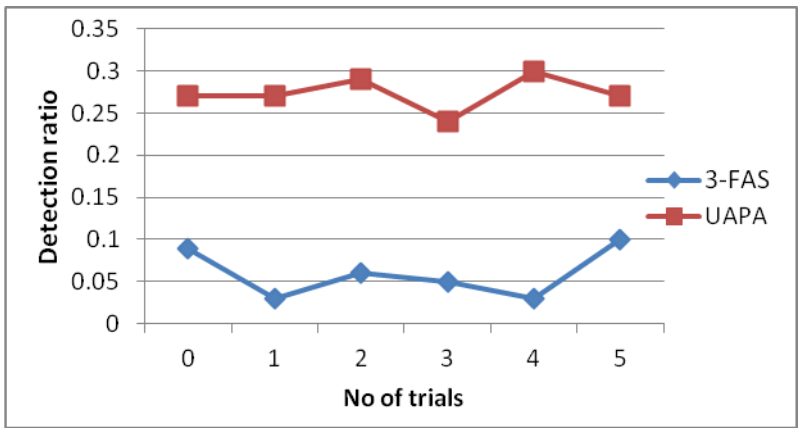

Figure 4. False Detection Ratio

Conclusion

For enhancing the network security and specific application's security three-factor substantiate mechanism with pattern ambiguity protection is proposed. The pattern ambiguity generates the hashing key for protecting the data and controls the user by the way of gateway node. The transaction code is generally included with private identification number with session keys like forward and reverse. 3-factor substantiate mechanism is ideally proposed and proves the detection and verification of sensor networks is better in transaction delay and in identification of false detection nodes.

References:

[1] Shen, B. H., Tiwari, A., Topol, Z., Chandra, H., Xu, S., Yadegar, J., & Luke, J. A. (2009, May). Proactive Trust Management System (PTMS) for trusted querying in wireless sensor networks. In *Intelligent Sensing, Situation Management, Impact Assessment, and Cyber-Sensing* (Vol. 7352, p. 735208). International Society for Optics and Photonics.

[2] M. Turkanovic´, B. Brumen, M. Hölbl, 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. 201231 (2014) 96–112.

[3] A.T.B. Jin, D.N.C. Ling, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognit. 37 (11) (2004) 2245–2255.

[4] M.L. Das, Two-factor user authentication in wireless sensor networks, IEEE Trans. Wirel. Commun. 8 (3) (2009) 1086–1090.

[5] L. Leng, A.T.B. Jin, M. Li, M.K. Khan, A remote cancellable palm print authentication protocol based on multi-directional two-dimensional palmphasor-fusion, Secur. Commun. Netw. 7 (11) (2014) 1860–1871.

[6] D. Wang, P. Wang, Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks, Ad Hoc Netw. 20 (2014) 1–15.

[7] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, H.-W. Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 11 (5) (2011) 4767–4779.

[8] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.