Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT TWO-FACTOR USER AUTHENTICATION PROTOCOL FOR AD-HOC WIRELESS SENSOR NETWORKS

V.S.SUDHAKARA RAO ANDE[1*], SREENIVASULU MERUVA[2]

[1]Research Scholar, Department of Computer science and Engineering, JNTU Ananthapur, 515002, India.
[2]Professor, Department of Computer Science and Engineering, KSRM College of Engineering, Kadapa ,516003, India.
*Corresponding Author: V.S.Sudhakara Rao Ande.

Email: andesudhakarrao@gmail.com

ABSTRACT

Providing access to confidential messages in a secured manner within Ad-hoc WSNs (Wireless Sensor Networks) is the challenging issue for researchers, due to lack of physical security and a greater number of potential attacks on the information transmitted through wireless radio. In 2021, Tsu-Yang et. al, presented a two-factor authentication protocol for Ad-hoc WSNs with the usage of smart card. It is an efficient scheme. This reduces the sensor node's energy usage while performing authentication of a user. It suffers from off-line password computation attack, the user un-traceability attack, password recovery attack. We realized that Tsu-Yang et. al's, scheme failed in real-time Ad-hoc WSN, where the information can be delivered in rigid time constraints. It also increases the burden on Gate Way Node (GWN) and leads to a denial-of-service attack. So, we present an authentication scheme that would be both effective and reliable, for Ad-hoc WSN to deliver information in a secured manner and in rigid time constraints. The security level of the protocol to be proposed is evaluated by the usage of Automated Validation of Internet Security Protocols and Applications (AVISPA) tool.
Keywords: *Ad-hoc WSN; Authentication Protocol; Gate Way Node, Rigid Time Constraint; Smart Card*.

1. INTRODUCTION

Ad-hoc WSNs are used for hostile environments and real-time applications [1-4] like traffic control, object tracking, agriculture, health, wildlife, and the battlefield, etc for continuous monitoring of surroundings. It has autonomous wireless nodes with a finite amount of memory, limited battery, and a low-speed processor. In the network, all the sensor nodes are controlled and coordinated by a centralized node called Gate Way Node (GWN).

[4] Sensor nodes collect data by monitoring surroundings, process the collected data, and transmit it to GWN. In the network, sensitive and confidential information is also transmitted from one sensor node to another through a wireless channel [4]. It is vulnerable to attacks against sensitivity and confidentiality of the transmitting information in wireless channel, due to lack of physical security. The vulnerable attacks are interception, masquerading, black hole attack, and SFA (Selective Forwarding Attack). An SFA is a severe attack. In this, the intruder can compromise a node in the network and drops selected packets transmitting packets through it. It breaks the continuity and quality of the received information. So, it needs to perform authentication of an agent, whenever try to chat with the sensor node either to request data or issue commands. The conventional security algorithms for user authentication are not fit for Ad-hoc WSN because of the mobility and resource constraints of sensor nodes [5]. So, we apply a lightweight authentication protocol to perform authentication of a user while accessing any sensor node. There are many authentication protocols developed for ad-hoc WSN. But they are delayed in do authentication of user. So, they are not suitable for Real-Time Applications.

In today's world, Ad-hoc WSNs are used mostly in Real-Time Application areas, where the collected information must be delivered within a specific time to do appropriate action at the proper time and solve the problem at an initial stage. For example, on the battlefield, it needs to know information regarding the position of opponents accurately, confidentially, and timely. Then only defeat the opponents.

Otherwise, if the information is delayed or it is intercepted or masquerades by opponents or intruders, it is not useful and leads to failure in the war. In this way, in Real-Time applications, the information received from the sensor node is useful only when it is delivered at a specific time and not affected by any intruder. So, it is a challenging issue to provide user authentication for access to a sensor node in Real-Time applications.

In this article, we present an authentication scheme to access sensor nodes in rigid time constraints. In this protocol, the senor node performs user authentication upon receiving a request from the user to initiate communication. The sensor node can use the user's credentials of the user received from GWN while authenticating a user. After authentication sensor node establishes and shares a session key using Elliptical Curve Cryptography (ECC) used to provide communication for the end of the session since ECC provides strong forward secrecy. This authentication protocol reduces the load on GWN and enables it to provide service to all the nodes without delay.

2. LITERATURE SURVEY

Wang. et al. [6] discussed a simple authentication scheme using passwords in WSN. It is implemented using only hash and EX-OR operations. But Tseng et al. [7] found, the protocol in [6] has the possibility of reply and forgery attacks. Das et al. [8] discussed authentication protocol and also key exchange protocol with the usage of smart cards for WSN. The user was authenticated at the Gateway node. However [9-11] found that Das's scheme was flawed and possible to incur security threats while doing the key exchange. But Vaidya et. al. [12] described an enhanced authentication scheme compare to Das's protocol.

Das et al. [13] and Xue et al. [14] discussed a pair of user validation and session key exchange schemes depend on the smart card. However, Turkanovic and Holbl[15] revealed that the authentication protocol in [13] also has security vulnerabilities. Li et al. [16] revealed that the protocol [14] suffers from many security threats and described an enhanced authentication protocol to prevent safety attacks for WSN. In 2013 Ohood et al. [17] presented a biometric-based authentication protocol. This protocol used the user's iris as a unique trait of the user to enhance the level of security. But it was suffering from security vulnerabilities. In 2014 Turkanovic et al. [18] discussed a dynamic protocol for authentication of the user and exchange of keys used in Ad-hoc WSN. In this user could directly authenticate at Gateway Node.

However, in 2016 Chang et al. [19] noticed that the protocol [18] was vulnerable to many security attacks (stolen smartcard attack, node capture, and node imitation attack), and revealed an authentication scheme based on the smart card for heterogeneous Ad-hoc WSN. It is a lightweight protocol, uses hash and EX-OR operations. However, Amin et al. [20] found that possible to incur off-line password finding attacks with smart card loss, user un-traceability attacks, smart-card recovery attacks, password change attacks and computation of previous session key attacks. In 2018 Amin et al. [20] proposed an authentication scheme based on the smart card to prevent active as well as passive security attacks in Ad-hoc WSN. However, Tsu-Yang Wu et al. [21] identified that the protocol not able to prevent compromise of key, forward security violation, user anonymity violation attacks. In 2021 Tsu-Yang Wu et al. [21] proposed an authentication scheme based on the smart card to prevent active as well as passive security attacks in Ad-hoc WSN. This protocol presents a new architecture of network model that enables the user to receive data directly from the sensor node through the Gate way node to reduce power usage of a sensor node and finally increases the durability of a node. It uses the fuzzy extractor technique for biometric enrollment. It may take more time for biometric generation and reproduction at the time of login. It may increase the load on GWN if more users and nodes are connected via GWN. The protocol [21] is not preferable In Real-Time networks, where the information should be received within the time limit. We present an authentication scheme that would be both effective and reliable, for Ad-hoc WSN to deliver information in a secured manner and in rigid time constraints. We also test the level of security using AVISPA tool. It is proved that out protocol has higher security and lower computational overhead compared to earlier.

Preliminaries

Communication/Network Model: Whenever the User Ui tries to access the sensor node Sj of Ad-hoc WSN, the authentication, and key exchange scheme can use the communication model as shown in the below Fig. 1.

Initially, a request for login is sent to sensor node Sj from the user Ui (1). Now, Sj sends a request to GWN for the login credentials of Ui (2). GWN sends the reply to Sj after performing authentication of Sj (3). Sj performs authentication of Ui and

Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

establishes session key agreement (4).

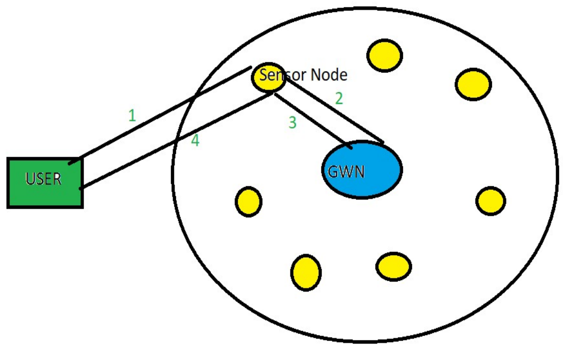

Figure 1 Communication Model

Model for Security: It describes the model for security using the AVISPA tool to validate and analyze the security provided by the authentication scheme [19]. AVISPA is used to measure the safety of the authentication schemes. It uses a formal language HLPSL (High-Level Protocols Specification Language), used to specify authentication schemes and the goals of security and saved with a file extension .HLPSL. It is specified in the form of roles.

3. METHODOLOGY

Here, we present a novel authentication scheme that rectifies the limitations of [21] authentication protocol. "There are five phases in the proposed protocol: pre-deployment phase, user registration phase, user log-in and authentication phase, password changing phase, and password recovery phase".

Table 1 List of Notations

U_i	The user
ID_i	The user U_i Identity
PW_i	The user U_i Password
SC_i	The smartcard of U_i
S_j	The sensor node
SID_j	The identity of S_j
f_j	The secret value of S_j
GWN	The gateway node
X_{GWN}	The GWN's long-term secret
X_{GWN-Ui}	The GWN and U_i shared
X_{GWN-Sj}	The GWN and S_j shared
T_1, T_2, T_3, T_4	The time stamps
ΔT	The expected transmission
$r_i, r_i', r_j, K_i, K_j, a, b$	The random numbers
SK	The shared session key
P	A point on the elliptic curve
P.x	The x-axis value of the point
‖,□,h()	The concatenation, XOR and Hash operations

a. ***Pre-deployment Phase***: Initially GWN generates a randomly long-term secret XGWN. Then, the GWN finds the secret fj=h(SIDj||XGWN), after that SIDj and fj are stored into the memory of the sensor node prior to deploying Sj into the network.

b. ***User Registration Phase*:** User Ui needs to register credentials at GWN to read data from the sensor node, then GWN checks the credentials of Ui and sends the smartcard to the user. The steps in the registration phase are described below (see Tab. 2).

Step1. Ui selects an identity IDi ,PWi and use random nonce ri, and calculates MPi=h(ri||PWi) and MIDi=h(ri||IDi) then send Send m1={MIDi,MPi} to GWN.

Step2. Now, GWN use random nonce ri' and Calculates MIi=h(MIDi||ri'), Fi=h(MIi||Xgwn) ,Ei=Fi+MPi and Send m2={Ei,MIi} new smartcard SCi to Ui through a secure channel.

Step3. After that, Ui computes Fi'=Ei+MPi ,HMPi=h(Fi||MIi||MPi), Ci=ri+h(IDi||PWi), Di=Fi+MPi , REC=PWi+h(IDi), and Stores MIi,HMPi,Ei,Ci,Di,REC into Smart Card SCi={ MIi,HMPi,Ei,Ci,Di,REC}

Table 2user Registration Phase

User Ui	***GWN***
Input ID_i,PW_i	
use random nonce r_i	
Compute the following	
MP_i=h(r_i‖PW_i)	
MID_i=h(r_i‖ID_i)	
Send m1={MID_i,MP_i} to GWN -- m1 ->	
	Received m1 from Ui
	use random nonce ri'
	Computes the following
	MIi=h(MIDi‖ri')
	Fi=h(MIi‖Xgwn)
	Ei=Fi+MPi

	Send m2={Ei,MIi} to Ui
Receives m2={E_i,MI_i} from GWN	**<---m2---**
Computes the following **F_i'=E_i+MP_i** **HMP_i=h(F_i||MI_i||MP_i)** **C_i=r_i+h(ID_i||PW_i)** **D_i=F_i+MP_i** **REC=PW_i+h(ID_i)** **Stores MIi,HMPi,Ei,Ci,Di,REC into Smart Card SCi={ MIi,HMPi,Ei,Ci,Di,REC}**	

*c. **Authentication and Key Exchange phase:***

In this GWN exchange the key of the current session for both user U_i and sensor node S_j (Tab.3).

Step1: Ui inputs the IDi,PWi at Terminal, it Calculates the following "ri'=Ci + h(IDi||PWi), MPi'=h(PWi||ri') , Fi'=Di+MPi', HMPi'=h(Fi'||MIi||MPi')". If HMPi'=HMPi then accepts the User and Computes the private key following by generating aarbitary nonce 'a' and Ki=a.P where P is a point on elliptic curve. Then computes "Yi=h(Fi'||T1), Zi=Ki+Yi, Ni=h(Yi||MIi||SIDj" and Send "m1={MIi,Zi,Ni,T1}" to Sj.

Step2: After receiving m1, Sjverify the consistency of time interval ie |T2-T1|<=ΔT. If it is false stops communication, otherwise computes "Aj=h(Fj||MIi||T2)" and send "m2={MIi,SIDj,Aj,T2,T1}" to GWN.

Step3: Now GWN verify the consistency of T2 i.e |T3-T2|<=ΔT. If it is false stops communication, otherwise computes Fj'=h(SIDj||Xgwn), Fi'=h(MIi||Xgwn), Aj'=h(Fj'||MIi||T2). If (Aj'=Aj) then accepts the Sensor and Computes the following Yi'=h(Fi'||T1), HYi=Yi'+h(MIi||Fj'), Hj=h(Fj'||T3) and Send m3={Hj,HYi,T3} to Sensor Sj.

Step 4: When Sj Receives m3= {Hj, HYi, T3} from GWN and verify the consistency of T3 ie |T4-T3|<=ΔT. If the condition is false stops communication, otherwise computes Hj'=h(Fj||T3). If (Hj'=Hj) then accepts GWN and Compute "Yi'=HYi+h(MIi||Fj), Ni'=h(Yi'||MIi||SIDj)", If (Ni'=Ni) then accepts User i and Computes the private key by select a random nonce 'b' and Kj=b.P, where P is a point on elliptic curve. It now computes Ki'=Zi+Yi', Rij=h(Ki'||T4)+Kj, EEi=h(Yi'||Ni'), SKj=h(abP.X), Send m4={Rij,EEi,T4} to Ui.

Step 5: Upon Receiving m4={Rij,EEi,T4} from S j and validates T4 ie |T5-T4|<=ΔT. If it is false stops communication, otherwise computes the following EEi'=h(Fi||Ni). If (EEi'=EEi) then accepts Sensor node and Computes the following Kj'=Rij+h(Ki||T4), SKi=h(abP.X) , where Ski is the shared session key. Produce a Random nonce ri and calculates MIDi'=h(ri||IDi) Send m5={MIDi',MPi,T5} to GWN.

Table 3 Authentication And Key Exchange Phase

*User^i*SCi={MIi,HMPi,Ei,Ci,Di,REC}	*Sensor j {Fj}*	*GWN {Xgwn}*
Inputs IDi,PWi at Terminal **Computes the following** **ri'=Ci + h(IDi||PWi)** **MPi'=h(PWi||ri')** **Fi'=Di+MPi'** **HMPi'=h(Fi'||MIi||MPi')** **If HMPi'=HMPi then accepts the User and Computes the following by generating a random nonce 'a' and Ki=a.P** **Yi=h(Fi'||T1)** **Zi=Ki+Yi** **Ni=h(Yi||MIi||SIDj** **Send m1={MIi,Zi,Ni,T1} to Sensor Node Sj**		

	Receives m1 from Useri and Checks the validity of T1 ie |T2-T1|<=ΔT. calculate Aj=h(Fj||MIi||T2) and m2={MIi,SIDj,Aj,T2,T1} to GWN	
		Receives m2={MIi.SIDj,Aj,T2,T1} and Checks the validity of T2 ie |T3-T2|<=ΔT. Computes the following Fj'=h(SIDj||Xgwn) Fi'=h(MIi||Xgwn) Aj'=h(Fj'||MIi||T2) If (Aj'=Aj) then accepts the Sensor and Computes the following Yi'=h(Fi'||T1) HYi=Yi'+h(MIi||Fj') Hj=h(Fj'||T3) Send m3={Hj,HYi,T3} to Sensor j

	**Receives m3={Hj,HYi,T3} from GWN and Checks the validate T3 ie |T4-T3|<=ΔT.
	Calculate Hj'=h(Fj||T3)
	If (Hj'=Hj) then accepts GWN and calculate the following
	Yi'=HYi+h(MIi||Fj)
	Ni'=h(Yi'||MIi||SIDj)
	If (Ni'=Ni) then accepts User i and Computes the following by select a random nonce 'b' and
	Kj=b.P
	Ki'=Zi+Yi'
	Rij=h(Ki'||T4)+Kj
	EEi=h(Yi'||Ni')
	SKj=h(abP.X)
	Send m4={Rij,EEi,T4} to Useri**	

Receives m4={Rij,EEi,T4} from Sensor j and Checks the validity of T4 ie |T5-T4|<=ΔT. and computes the following EEi'=h(Fi||Ni) If (EEi'=EEi) then accepts Sensor node and Computes the following Kj'=Rij+h(Ki||T4) SKi=h(abP.X) Generates a Random nonce ri Compute the following MIDi'=h(ri||IDi) Send m5={MIDi',MPi,T5} to GWN		
		Received m5={MIDi', MPi', T5} from Useri

		and check the Validity of T5 ie |T6-T5|<=ΔT. Computes Fi=h(MID'||Xgwn) If(Fi=Fi') then accept User i and Generates a random nonce ri' Computes the following MIi'=h(MIDi'||ri') Fi'=h(MIi||Xgwn) Ei'=Fi'+MPi Send m6={Ei',MIi',T6} to Useri
Receives m6={Ei',MIi',T6} from GWN and check the Validity of T5 ie |T7-T6|<=ΔT. Computes the following Fi=Ei'+MPi If (Fi'=Fi) then accepts GWN and computes the following HMPi'=h(Fi||MIi'||MPi) Ci'=ri'+h(IDi||PWi) Di'=Fi+MPi Replace MIi',HMPi',Ei',Ci',Di' into Smart Card SCi={ MIi',HMPi',Ei',Ci',Di',REC}		

Step6: GWN Receives m5= {MIDi',MPi',T5} from Ui and check the Validity of T5 ie |T6-T5|<=ΔT. If it is false stops communication, otherwise Computes Fi=h(MID'||Xgwn). If(Fi=Fi') then accept Ui and a random nonce ri' is generated. Computes the following MIi'=h(MIDi'||ri'), Fi'=h(MIi||Xgwn), Ei'=Fi'+MPi and Send m6={Ei',MIi',T6} to Ui.

Step7: Ui after receiving m6={Ei',MIi',T6} from GWN and check the Validity of T5 ie |T7-T6|<=ΔT. If it is false stops communication, otherwise Computes the following Fi=Ei'+MPi. If (Fi'=Fi) then accepts GWN and computes the following HMPi'=h(Fi||MIi'||MPi) , Ci'=ri'+h(IDi||PWi), Di'=Fi+MPi , Replace MIi',HMPi',Ei',Ci',Di' into Smart Card as SCi={ MIi',HMPi',Ei',Ci',Di',REC}.

d. asswordRecovery Phase

AnyU$_i$executesthisphase when maynot be able to recollectthepassword. First, U$_i$enter the IDi , after the smart card has been inserted, then Computes the followingPWi'=REC+h(IDi), Fi'=Ci+h(IDi||PWi'), MPi'=Ei+Fi', HMPi'=h(Fi'||MPi'). If (HMPi'=HMP) then accepts the user and returns the PWi' to U$_i$ as shown in Tab. 4.

Table 4 Password Recovery Phase

Inserts the smart card and enters the IDi
Computes the following
PWi'=REC+h(IDi)
Fi'=Ci+h(IDi||PWi')
MPi'=Ei+Fi'
HMPi'=h(Fi'||MPi')
If (HMPi'=HMP) then accepts the user and returns the PWi' to the user

e. Password Change Phase

It is required to execute this phase frequently to modify the password for hygiene security. The ability to changethepasswordwithout the involvement of the gatewaynodeisa needfulrequisite of the sensor node to minimize network traffic. This phase is described asshown in Tab. 5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Initially, Ui inserts the Smart card and enters IDi, PWi at the user terminal. Now the terminal computes the followingFi'=Ci+h(IDi||PWi), MPi'=Ei+Fi', HMPi'=h(Fi'||MPi'). If HMPi'=HMPi) then accepts the user and prompt for new password PWi', now computes ri=Di+ h(Fi'||MIi), MPi'=h(ri'||PWi'), Ei'=Ei+MPi+MPi', REC'=PWi'+h(IDi), HMPi'=h(FI'||MIi||MPi'), Di'=ri'+h(Fi'i||MIi), Ci'=Fi'+ h(IDi||PWi'). Finally replace Ei,REC,HMPi,Ci,Di with Ei',REC',HMPi' ,Ci',Di' in the smart card as SC'={ MIi,HMPi',Ei',Ci',Di',REC'}.

Table 5 Password Change Phase

Inserts the Smart card and enters IDi.PWi at user
Now computes the following
Fi'=Ci+h(IDi||PWi)
MPi'=Ei+Fi'
HMPi'=h(Fi'||MPi')
If HMPi'=HMPi) then accepts the user
and prompt for new password PWi'
ri=Di+ h(Fi'||MIi)
MPi'=h(ri'||PWi')
Ei'=Ei+MPi+MPi'
REC'=PWi'+h(IDi)
HMPi'=h(FI'||MIi||MPi')
Di'=ri'+h(Fi'i||MIi)
Ci'=Fi'+ h(IDi||PWi')
Replace Ei,REC,HMPi,Ci,Di with Ei',REC',HMPi'
SC'={ MIi,HMPi',Ei',Ci',Di',REC'}

4. RESULTS: SIMULATION OF PROTOCOL IN AVISPA TOOL

The simulation of the described protocol has been discussed in this section with the use of the AVISPA tool. It is a general security evaluation tool. It is used to check that the given protocol is secure or insecure. It is referred for the interested reader to [22-24] for detailed information regarding HLPSL and also the AVISPA tool.

4.1 *Specification of Presented Protocol in HLPSL*

Here, we elaborate on how to simulate the proposed protocol in brief for agents played by Ui, S j, and GWN, goal, session, and the environment. In HLPSL specification the following security and authentication propositions are used.

1. Secret (IDi', subs1, {Ui, Sj, GWN}): This means, the IDi of user Ui was only known by Ui, Sj, and GWN. However, If an adversary knows IDi of the user, then possible to reveals the anonymity of the user.
2. Secret ({PWi}, subs2,{Ui}): Means that only Ui, had know the PWi of Ui. However, If the adversary will know IDi, then try to impersonate the user Ui.
3. Secret ({SKi'}, subs3,{Ui,Sj}) : Means that only Ui as well as Sj had aware the Ski' of user Ui. However, If an adversary will know Ski', then try to break the forward secrecy of the user and sensor node.
4. Secret ({Xgwn'}, subs5, {GWN}): Means that only GWN had to know the Xgwn' of Ui. However, If the adversary will know Xgwn', then try to impersonate the user GWN.
5. Witness (Ui,Sj,user_sensor,Ki') : states that user Ui has randomly generated number Ki' for the sensor Sj.
6. Witness (Sj, Ui, sensor_user, Kj'): This means that sensor Sj has generated the random number Kj' for the user Ui.
7. Request (Ui, Sj, pserver-Alice, B'): The user Ui has been strongly authenticates the Sensor S j depends on the message B'.

4.2 *Execution of Simulation*

We run the HLPSL code on the Span tool downloaded from http://www.avispa-project.org and installed it on ubuntu14.04. Upon successful execution of the code, AVISPA had a display that describes the given protocol as secure or insecure concerning the On_the_Fly_Model_Checker (OFMC) and Constraint_Logic_based_Attack Searcher (CL-AtSe) models (Fig. 2, Fig. 3). Alternatively, the proposed protocol protected from both active attacks as well as passive attacks. The properties of secrecy and authenticity are fulfilled by the protocol. Hence, we state that the described protocol provides strong security.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/avss1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 145.58s
  visitedNodes: 34225 nodes
  depth: 6 plies
```

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 2: Results Of Simulation After Executed In OFMC

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL

/home/span/span/testsuite/results/avss1.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
 Analysed  : 90 states
 Reachable : 90 states
 Translation: 0.12 seconds
 Computation: 2.15 seconds
```

Figure 3 Results Of Simulation After Executed Inofmc Model CL-Atse Model.

5. SECURITYANALYSIS OF PROTOCOL

Hypothesis 1: The described protocol furnishes security from stolen smartcard attacks

Proof: This type of attack seeks to get credential information with information that could be retrieved from the smartcard [21, 22]. The adversary tries to obtain IDi and PWi of user Ui and secretes information of GWN and Sj also.

The adversary retrieves SCi={ MIi,HMPi,Ei,Ci,Di,REC} from the stolen smart card, where MIi=h(MIDi||ri'), HMPi=h(Fi||MIi||MPi), Ei=Fi+MPi, Ci=ri+h(IDi||PWi), Di=Fi+MPi, REC=PWi+h(IDi) using this adversary unable to obtain IDi, PWi of user Ui, a one-way hash function protects them using Ci=ri+h(IDi||PWi).

GWN's secret key XGWN is only used in Fi=h(MIi||Xgwn), Ei=Fi+MPi, Where MPi=h(ri||PWi) and ri=Ci+h(IDi||PWi). So, it is a challenge for the adversary to obtain the secrete key of GWN.

If the legal user Ui is going to act for malicious purposes (i.e. insider threat) and is trying to get GWN's secret key X_{GWN}, No one malicious user can derive GWN,s secret key, even though Ui knows fi = h(MIi ‖ XGWN) and MIDi, where MIi = h(MIDi ‖ ri'), Ui is still not able to extract XGWN because h(·) is non-invertible.

Hypothesis 2: The protocol presented provides security from off-line identity predicting attacks.

Proof: It needs to keep user identity safe from the adversary, to maintain the confidentiality of the user. To break the user's anonymity, an adversary may try to know user Ui's IDi with the usage of either the smartcard or the protocol. In Hypothesis 1, we have shown that IDi cannot be derived from data collected from the smart card. Furthermore, IDi cannot be derived from public data by implementing the scheme for the following reasons:

We assume that adversary intercepting the message after login {MIi, Zi, Ni, T1}, where Ni=h(Yi||MIi||SIDj), MIi=h(MIDi||ri'), Zi=Ki+Yi.Note that MIi is protected by h(·) and (MIDi, ri), where ri is a randomly generated number. Because of h(.)'s One-Way property, the adversary is unable to extract(MIDi, ri). Moreover, an adversary is unable to guess IDi using MIi without the knowledge of ri. Now, the adversary is unable to know IDi.

Hypothesis 3: The described protocol furnishes security from un-traceability.

Proof: Un-traceability means it is not possible to tracked or identified Ui with the usage of the exchanged messages, In an anonymous authentication system. This functionality is set out in step6 and step7 of the authentication phase of our protocol. In each session, MIi has been modified just whenever the exchange of the current session key takes place. Remind that the responses of both login as well as authentication in this scheme are unique because of the use of random numbers as well as timestamps.

Hypothesis 4: The described algorithm is secure from the attacks of determining passwords by executing offline modules.

Proof: In general users always select a low potential for the purpose of comfort, password from a small dictionary. It makes easier to conduct password guessing attack in offline mode in a polynomial time. In hypothesis 1, we described that unable to determine the Ui's password PWi even though have access to the smartcard of the user.

In addition, both username and password and auth entication responses are PWi individual.

Consequently, accessibility to all these responses doesn't help in the determination of PWi.

Hypothesis 5: The described protocol is safe from user imitation attacks.

Proof: In this, the attacker mainly monitors an earlier message used to log in, and then tries to fabricate a fresh login message authenticated using GWN. Our protocol is secure from such types of

attacks.
We suppose that adversary have been access to an earlier message of login {MIi, Zi, Ni, T1}, where Ni=h(Yi||MIi||SIDj), MIi=h(MIDi||ri'), Zi=Ki+Yi. Even though the adversary can select a randomly generated number Ki and read the present timestamp T1, unable to know fi, SIDj, MIDi. Therefore, the Adversary is unable to find the valid message for login.

Hypothesis 6: The described scheme is safe from gateway imitation attacks.

Proof: As a part of imitating the GWN, the adversary needs to send a fabricated response similar to compare with the GWN's response. Suppose that adversary reads {Hj, HYi, T3} from the public channel, where Hj=h(Fj'||T3), HYi=Yi'+h(MIi||Fj'). Since confidential (unknown) information fj used for compute both Hj and HYj, the adversary is unable to compute Hj and HYj without fj.

Hypothesis 7: The described scheme is safe from imitation of sensor node attacks.

Proof: In Ad-hoc WSN, it is more precious to prevent imitation of sensor node for the purpose of preventing the access of unauthorized users. In the described protocol, the adversary tries to imitate Sj with the creation of a forged response that is similar to compare with Sj's response. Guess, theadversary knows {MIi,SIDj,Aj,T2,T1} , where Aj=h(Fj||MIi||T2) and {Rij,EEi,T4} where Rij=h(Ki'||T4)+Kj, EEi=h(Yi'||Ni').Now, the adversary tries to compute a forged authentic message. But adversary requires fj, Yi, and Ki. Since the adversary does not know fj, Yi, and Ki. Hence, the described protocol is safe from node imitation attacks.

Hypothesis 8: The protocol described here is safe from advantaged malicious user attacks.

Proof: it is believed that the corrupt/malicious inside user has been accessed the password of another valid user and tries to mimic that valid user. In the described protocol during the phase of user registration, the Ui did not send PWi through a public channel. So, PWi is not revealed to any insider of WSN, and not possible to implement malicious user attacks.

Hypothesis 9: The protocol described is safe from computing the key of current or earlier session attacks.

Proof: To avail a safe communication between entities in the network, the message exchanged between the two entities is encrypted using a session key. The encoded data is sent via an unsafe channel. The property of freshness is compulsorily fulfilled by the key of the current session. In this protocol, the key of current session SK=h(abP.X) (where Ki=a.P and Kj=b.P, P is a point on an elliptic curve, and a,b are random numbers) is exchanged between Ui and Sj. Noticed that the safety for the key of the current session is based on Ki, Kj unknown to the adversary. So, the adversary is unable to compute the key of the current session. We also remember that the usage of random numbers Ki and Kj avails the property of freshness in the key of the current session.

Hypothesis 10: The protocol described is providing security from attacks of session-specific data that is already known.

Proof: In these attacks, the adversary tries to calculate the key of a further session using random numbers for a limited period of time. Our protocol, on the other hand, states that the key of each session is calculated using SK=h(abP.X). Assume that the adversary obtains Ki or Kj and also calculate another random number with the random number learn first (e.g.Kj with Ki, and also vice versa). Notice that the session's secrecy depends on P. Since P is unknown to the adversary, the adversary is unable to compute the key.

Hypothesis 11: The protocol described furnishes validation of the key of a session.

Proof: In the proposed protocol, S j will calculate the key of a session SKj after authenticating the GWN and also Ui successfully. Similarly, the Ui verifies the key of a session. Hence, the proposed protocol has enabled the key validation of a session.

Hypothesis 12: The scheme described facilitate authentication mutually.

Proof: In the running of our scheme, every agent validates all the other agents. In the phase of authentication, GWN verifies Ui and also Sj in Step 3. Sji verifies GWN and also Ui in step4. In Step 5, Uij verifies the authentication of Sj and also GWN using the data arrived. Finally, Ui authenticates GWN and also Sj in the 7th Step. Hence, the described scheme provides authentication mutually.

6. COMPARISON AND EVALUATION OF PERFORMANCE

Now discuss a relative work of described authentication scheme with some existing protocols, in correspondence to privileges of security (shown in Tab. 6), calculation costs (shown in Tab. 7), also Costs of storage and interaction (shown in Tab. 8).

The protocols mentioned in Table 6. In [12, 13, 14, 16, 19, 20, 21] are vulnerable to security attacks. Moreover, the protocols in [12, 13, 14, 16, 19] does not provide recovery of password.

The calculation cost in both users, sensor node modules in the proposed scheme is a little bit more than existed schemes, to provide un-traceability of user and also verify the key of a session in the presented scheme. Moreover, the GWN calculation cost in the proposed scheme is lesser compare to [12, 13, 14, 16, 19, 20, 21]. In other words, the gateway node of the proposed protocol performs fewer computations. Since user authentication performs at the sensor node. So, there is the mitigation of denial of service attack (if adversary intentionally sends login and authentication messages with incorrect details to makes the gateway node as busy and improve the congestion in the network, finally blocks the gateway node from providing service to genuine users) and enable the gateway node to provide on-time service to users and sensor nodes.

To formally evaluate the cost of communication, we consider that the size of a password, random number, hash function, identity is 128 bits correspondingly. The presented protocol is also supposed to use asymmetric cryptography to get the encrypted message of 128 bits length. In the work of comparison, we display the size of the data (bits) which an agent has been sending or receive. Suppose, (512/640) describes that a sensor node has sent 512 bits and also receives 640 bits in every session. It is noticed by looking at Table. 8 the cost of communication in sensor nodes is not more compares to existed schemes. Moreover, the schemes described have less cost of communication for the gateway node. Hence, the protocol described is much effective in comparison to existed schemes in view of mitigation of denial of service (DOS) attacks provide on-time service to users and sensor nodes.

Table 6 A Summative Reports For A Comparison Of Security Privileges

Authentication scheme	Tur-Hol [12]	Das [13]	Xue [14]	Tur [16]	Chang [19]	Ruhul [20]	Tsu-Yang Wu[21]	Presented
Prevent Anonymity of the user	N	N	N	N	Y	Y	Y	Y
Prevent Anonymity of the sensor node	N	N	N	N	Y	N	Y	Y
Prevent Un-traceability attack	N	N	N	N	N	Y	N	Y
Prevent Excepting password attack	Y	N	N	N	N	Y	N	Y
Prevent Legitimate insider attack	Y	N	N	Y	Y	Y	Y	Y
Prevent Data threaten checker attack	Y	Y	Y	Y	Y	Y	Y	Y
Prevent Threaten smartcard attack	N	N	N	N	N	Y	N	Y
Prevent Imitation attack	N	N	N	N	Y	Y	Y	Y
Prevent Session specific data attack	N	Y	N	N	Y	Y	Y	Y
Allow Addition of node dynamically	N	Y	Y	Y	Y	Y	Y	Y
Allow Authentication mutually	N	N	N	N	Y	Y	Y	Y
Allow Validation of session key	Y	Y	Y	Y	N	Y	Y	Y
Allow Reset of Password	Y	Y	Y	Y	Y	Y	Y	Y
Allow Recovery of smartcard	N	N	N	N	N	Y	Y	Y
Allow Revocation of password	N	N	N	N	N	Y	Y	Y
Allow Simulation using AVISPA	N	N	N	N	N	Y	Y	Y

Y: mention that the authentication scheme prevents the specified attack;
N: mention that the authentication scheme may suffer from the specified attack

Table 7A Summative Reports For A Comparison Of The Complexity Of Calculations
T_h and T_{xor} be The Time For Performing A Hash Operation And XOR Operations Respectively.

Authentication scheme	**User**	**Sensor Node**	**GWN/BS**
Das [13]	**($5T_h$+ $1T_{xor}$)**	**(-)**	**($5T_h$+ $4T_{xor}$)**
Xue [14]	**($7T_h$)**	**($6T_h$)**	**($13T_h$)**
Tur [16]	**($7T_h$)**	**($5T_h$)**	**($7T_h$)**
Chang [19]	**($7T_h$+$4T_{xor}$)**	**($5T_h$+$4T_{xor}$)**	**($9T_h$+$1T_{xor}$)**
Ruhul [20]	**($14T_h$+$10T_{xor}$)**	**($4T_h$+$3T_{xor}$)**	**($17T_h$+$7T_{xor}$)**
Tsu-Yang Wu [21]	**($11T_h$+$10T_{xor}$)**	**($6T_h$+$3T_{xor}$)**	**($14T_h$+$7T_{xor}$)**
Proposed	**($10T_h$+$4T_{xor}$)**	**($5T_h$+$2T_{xor}$)**	**($6T_h$+$1T_{xor}$)**

Table 8 A Summative Reports For A Comparison Of Storage Complexity And Communication Complexity

Authentication scheme	SNCS	UECS	GWN
Das.[13]	-----	[384,384]	[384,384]
Xue [14]	[512,640]	[768,512]	[640,1280]
Tur [16]	[1792,1408]	[640,768]	[768,1024]
Chang [19]	[1152,512]	[512,384]	[512,768]
Ruhul [20]	[384,512]	[896,768]	[1280,1280]
Tsu-Yang [21]	[640,512]	[768,384]	[640,768]
Proposed	**[384,512]**	**[384,512]**	**[384,640]**

SNSC: cost of communication for Sensor node (bits); **UECS**: cost of communication for User (bits);
GWN: cost of communication for Gateway node (bits); **(m,n)**: transmitted m-bit messages and received n-bit messages.

7. CONCLUSION

This work reviewed protocols proposed by and also identified limitations of security. We proposed an efficient, effective, and novel authentication scheme for implementation in Ah-hoc WSN that has a highly reliable gateway node. We also presented a novel authentication scheme against the vulnerabilities in providing security noticed in authentication schemes also evaluate the safety against security attacks in the presented authentication scheme with the usage of a protocol simulation tool called AVISPA. The summative report of comparison of existed authentication schemes with the proposed one describes that presented authentication scheme has lesser calculation and data exchange cost with a more effective and efficient level of security. Future work may incur deployment of the presented authentication scheme in a distributed network like Ad-hoc WSN comprises multiple gateway nodes for validating the security of the authentication scheme in the scope of Ad-hoc WSN with more than one gateway node.

REFERENCES

[1] M. L. Das, "Two-factor user authentication in wireless sensor networks,"IEEE *Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[2] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[3] T.H. Chen and W.K. Shih, "A robust mutual authentication protocol for wireless sensor networks," ETRI *Journal*, vol. 32, no. 5, pp. 704–712, 2010.

[4] B. Vaidya, D. Makrakis and H. T. Mouftah, "Improved twofactor user authentication in wireless sensor networks," IEEE *6th International Conference on Wireless and Mobile Computing, Networking and Communications*, vol. 3, no. 5, pp. 600–606, 2010.

[5] K. H. M.Wong, Y, J. Cao and S.Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sens. Netw. Ubiq. Trustworthy Comput*., vol. 1, pp. 244–251, 2006.

[6] F. Wang, Y. Zhang, Y. Xu, L. Wu and B. Diao, "A dos-resilient enhanced two-factor user authentication scheme in wireless sensor networks," in *2014 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1096– 1102, 2014.

[7] H. R. Tseng, R. H. Jan andW. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," Proc. *IEEE Global Telecommun. Conf*., , pp. 986–990., 2007.

[8] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun*., vol. 8, no. 3, pp. 1086–1090, 2009.

[9] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2450–2459, Mar. 2010.

[10] 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, 2010.

[11] 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.WirelessNetw.*, vol. 10, no. 4, pp. 361–371, 2010.

[12] B. Vaidya, D.Makrakis and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," Proc. *IEEE 6th Int. Conf. Wireless Mobile Comput. Netw. Commun*., pp. 600–606, 2010.

[13] 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, 2014.

[14] 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, 2013.

[15] 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.

[16] C. T. Li, C. Y. Weng and C. C. Lee, "An advanced temporal credentialbased security scheme with mutual authentication and key agreement for wireless sensor networks," *Sensors*, vol. 13, no. 8, pp. 9589–9603, 2014.

[17] OhoodAlthobaiti, Mznah Al-Rodhaan and Abdullah Al-Dhelaan "An Efficient Biometric Authentication Protocol for Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, Volume 2013, Article ID 407971, 13 pages.

[18] 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, 2014.

[19] Chin-Chen Changand Hai.-Duong. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks", *IEEE Transactions on Wireless Communications*vol. 15, no. 1, pp. 357–366, 2016.

[20] Ruhul Amin, SK Hafizul Islam, Neeraj Kumar, Kim-Kwang and Raymond Choo, "An Untraceable and Anonymous Password Authentication Protocol for Heterogeneous Wireless Sensor Networks ", *Journal of Network and Computer Applications*Volume 104, 15 February 2018, Pages 133-144.

[21] Tsu-Yang Wu , Lei Yang , Zhiyuan Lee , Shu-Chuan Chu , Saru Kumari and Sachin Kumar," A Provably Secure Three-Factor Authentication Protocol for Wireless Sensor Networks,"*Hindawi ,Wireless Communications and Mobile Computing* Volume 2021, Article ID 5537018, 15 pages

[22] AVISPA. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispa-project.org/(accessed on 4 December 2020).

[23] SPAN: A Security Protocol Animator for AVISPA. Available online: http://www.avispa-project.org/ (accessed on 4 Decem-ber 2020).

[24] Dolev, D.and Yao, A. On the security of public key protocols. IEEE Trans. Inf. Theory 1983, 29, 198–208. [CrossRef]