A Secure Authentication Protocol for Vehicular Ad-Hoc Networks

Preeti Chandrakar
Department of Computer Science and Engineering,
NIT Raipur, India – 492010
pchandrakar.cs@nitrr.ac.in

Ayush Jain
Department of Computer Science and Engineering
NIT Raipur, India – 492010
ayushjain17aug@gmail.com

Sandeep Balivada
Department of Computer Science and Engineering
NIT Raipur, India – 492010
sandeepbalivada123@gmail.com

Rifaqat Ali
Department of Computer Applications
Madanapalle Institute of Technology & Science
Madanapalle, India-517325
rifaqatali27@gmail.com

***Abstract*—The recent developments in industry of vehicles and technology based on wireless communication, has led to tremendous progress in vehicular ad-hoc networks. Using the Wireless Sensor Networks (WSNs), the user can get a lot of traffic information like traffic congestion, average speed of vehicles on road, accidents if any occurred, etc. by the network. But these networks also become vulnerable if proper security mechanisms are not put into place. The prime motive behind taking up this project was to try and contribute in the development of such security protocol so that no one can illegally interfere with these networks. Many different security authentication protocols have been made previously but they suffer from one or the other disadvantage. After detailed and thorough reading and analysis of these protocols and their shortcomings,effort has been made to devise a better protocol from these existing ones.**

Further, the proposed scheme has been simulated using the widely used"Automated Validation of Internet Security Protocols and Applications" (AVISPA) tool.It makes sure that the protocol is safe from the active and passive attacks and also prevents the replay, man-in-the-middle attacks and various other kinds of attacks. The complete security analysis of the protocol has been done in the presented paper. Also the performance evaluation done on the proposed scheme shows that the given protocol is extremely secureand also has a better complexity in terms of communication cost, estimated time and computation cost.

Keywords—Authentication, AVISPA, VANETs, Security, SHA.

I. INTRODUCTION

A. Vehicular Ad-hoc Networks (VANETs)

VANETs use vehicles as mobile nodes and could be defined as a subdivson of mobile ad hoc networks (MANETs) which provide communication channel between mobile vehicles and the roadside units (RSUs) but also differ largely from different networks because of their own unique characteristics like dynamicity. If the necessary details about the road is known, future position of a vehicle could be predicted. In broad sense it could be said that the network is dynamic in terms of time and space.

B. Security

Security in streets has become a serious issue for authorities and vehicle manufacturers in the recent decades. The total number of vehicles in the world has risen tremendously, thus increasing the activities in the network and creating more unwanted happenings.Thus being affected by this situation, the industries involved in car manufacturing and telecommunication businesses have began attachingwireless devices to vehicles for interconnection. Communication between cars or the roadside units helps in improving driving safety and exchanging traffic information. Providing security and privacy has come out as the two major challenges within the infrastructure of VANETs. Authentication between all the different parties is required but in contrast, no one wants to reveal his/her real. One may send some wrong messages or pretend like others to send messages. The aim/goal of VANET includes auto crash prevention, more secure streets and clog decrease etc.

C. Our Contribution

The main contributions are:

- It has been shown that the existing protocol suffer from many shortcomings which we have tried to overcome in our protocol.
- The protocol is verified using the AVISPA tool and thus shown that it successfully mutually authenticates thevarious components namely the user, sink and the vehicle sensor.

978-1-5386-8158-9/19/$31.00 2019 IEEE

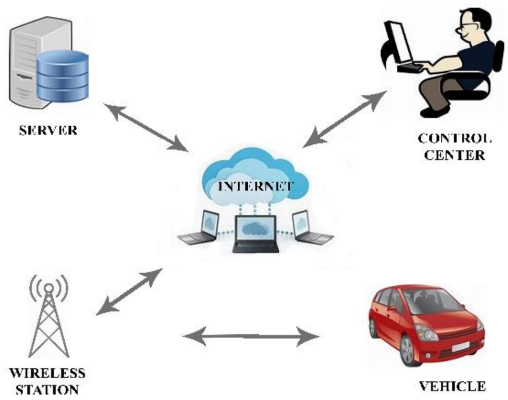

Fig 1 - Network Model of VANETs

II. RELATED STUDY

In the field of security and secrecy in ad hoc networks a number of research works have been done by a lot of researches and numerous protocols have been proposed. In the authentication protocol proposed by Amin and Biswas[26],three phases:- registration, login and authentication phase are present for their VANET. It has been found out that their scheme is prone to different kinds of attacks such as unauthorized message access attacks, smart access card stolen attack, replay attack etc. The registration message that has been generated in the previous phases is being left without taking any security measures. If some unauthorized person tries to access that RM through the insecure channel, then most probably he gets succeeded in doing so as the registration message is not secured.

He and Xu together proposed a scheme for VANETs [3] that is based on identities and is very efficient. Elliptic Curve Cryptography(ECC) is the main base for their ID based scheme.A point O generates an additive group H of order q on a elliptical curve D: y2 – x3 + ux+ v mod p that is non-singular. p,q are two prime numbers of 160 bit each and u,v belongs to Z * p.This Elliptic Curve Cryptography approach is very difficult to use and so a better, simple and more secured authentication protocol is to be proposed. This has been done in the proposed scheme. A sound and effectivescheme has been proposed by Islam, Obaidat and Reddy [6]. It is a privacy preserving scheme based on passwords.They found out that the protocols that are implemented using elliptic curve or the bilinear pairing are very time consuming. A hash function has less execution time and is less costly when compared to the costs of numerous operations of elliptical curves. To overcome all these existing attacks they proposed a robust CPPA protocol. But the same registration message security is not considered in this protocol.

This research paper introducesasecure mechanism for wirelessnetworks in VANETs to solve these drawbacks. Research papers done by Chandrakar and Om on cryptanalysis [7-19]are referred for necessary information.

III. PROPOSED SCHEME – ALGORITHM FOR VANETS

A. *Smart Access Card (SAC) Generation & Registration phase:*

1) User has – a) UID
b) PWD

2) User generates a random nonce RN_u by user using random number generator function.

3) After this, the user calculates the hash values of UID and PWD as HUID and HPWD by appending each with RN_u and hashing them using SHA (Secured Hashing algorithm) :-

$HUID = h\ (UID \,||\, RN_u)$

$HPWD=h\ (PWD||RN_u)$ → Phase 1

4) Send **<HUID, HPWD>**to sink node through a secured channel.

5) Now at the sink node, a random nonce RN_s is generated using the random number generator function.

6) Concatenate both HUID and HPWD with RNs and hash with SHA to produce the Registration message RM :-

$RM = h\ (HUID||HPWD||RN_s)$

7) Calculate the value SN by hashing concatenation of K_s and HPWD (sink node key):-

$SN=h(K_s) \oplus h(HPWD) \oplus h(RN_s)$ → Phase 2

8) Store the values SN, RM, RN_s from phase 2 in the highly secured Smart Access Card (SAC).

9) SAC is delivered to the Registered User.

10) The user then computes HN_u on his own by using his UID, PWD and RN_u that are only known to him :-

$HN_u = h\ (UID \,||\, PWD) \oplus RN_u$

11) Store HN_u in SAC → Phase 3

---------------- Registration phase completed -----------------

Output: - User registration successful.

SAC contains details of SN, RM, RN_s, HN_u.

User possesses SAC.

Explanation:

User has his own unique User-ID UID and password PWD. It generates a random nonce RN_u for user using rand function. In the first phase it calculates hash values of UID and PWD as HUID and HPWD by appending each with RN_u and hashing them using SHA (Secured Hashing algorithm).Then a random nonce RN_s for sink using rand function is generated.

Both HUID and HPWD are concatenated with RN_s and hashed with SHA to produce the Registration message RM. After this, the value SN is calculated by hashing concatenation of K_s and HPWD (sink node key). Then the sink node stores the values of SN, RM, RN_s from phase 2 in the highly secured

Smart Access Card (SAC) and deliver it to the registered user. The user then computes HN_u on his own by using his UID, PWD and RNu that are only known to him. This HNu is also stored in the SAC. With this the registration of the user gets completed successfully and he has the SAC with the details of SN, RM, RNs, HNu.

Fig 2 - Smart Card Mechanism

B. Login phase

1) User enters – a) UID^e
b) PWD^e

2) The random nonce RN_u for user is recalculated using UID^e, PWD^e and HN_u (stored in SAC) :-
$RN_u = h\ (UID \parallel PWD) \oplus HN_u$

3) Now the user calculate $HUID^e$ and $HPWD^e$ by appending UID^e and PWD^e with RN_u and hashing them using SHA (Secured Hashing algorithm) :-
$HUID^e = h\ (UID^e \parallel RN_u)$
$HPWD^e = h\ (PWD^e \parallel RN_u)$

4) User concatenates both $HUID_e$ and $HPWD_e$ with RN_s and hash with SHA to produce the Registration message RM_e.
$RM_e = h\ (HUID \parallel HPWD \parallel RN_s)$

5) User checks whether $RM = RM_e$?

6) User calculates Mt_s by hashing concatenation of values SN, RM and UN_u :-
$Mt_s = h\ (SN \parallel RM \parallel UN_u)$

7) User then calculates P1 by XORing the value of SN with UN_u:-
$P1 = SN \oplus UN_u$

8) Calculates P_2 by XORing hash value of ID_k (Identity of Kth vehicle sensor)and hash value of concatenation SN and P_1 :-
$P_2 = ID_k \oplus h\ (SN \parallel P_1)$

9) Calculates P_3 by XORing value RM and RN_s :-
$P_3 = RM \oplus UN_u$

10) Send Mt_s, P_1, P_2 and P_3 via insecure channel to sink node.

Explanation:

After the completion of registration phase, the user can login to the system to access the network. In the login phase the user enters his User-Id UID and Password PWD. Random nonce RN_u for user is recalculated using UID^e, PWD^e and HN_u that are stored in SAC. Now $HUID^e$ and $HPWD^e$ are calculated by appending UID^e and PWD^e with RN_u and hashing them using Secured Hashing Algorithm. Concatenate both $HUID^e$ and $HPWD^e$ with RN_s and hash with SHA to produce the Registration message RM^e . Now, the registration message RM is checked whether it is equal to the previous Registration Message RM. If they both match then the further process is continued or else it is discarded and prevented from doing further process. Then generate a random nonce N_u and calculate Mt_s by hashing concatenation of values SN, RM and N_u .Calculate P_2 by XORing hash value of ID_j (Identity of J_{th} sink node) and hash value of concatenation SN and P_1. Then calculate P_3 by Xoring values of RM and UN_u. Finally all the values M_{ts}, P_1, P_2, P_3 are sent via insecure channel to sink node. With this the login phase is completed and the most important authentication phase to establish a session starts.

C. Authentication Phase- 1(In sink node)

Authentication phase starts right after the completion of login phase. This phase takes place in three important sub-phases. The authentication phase 1 takes place at Sink node. All the authentication requirements at this phase are dealt here.

1) Calculate UN_u by XORing SN^e and P_1 :-
$UN_u^e = SN^e \oplus P_1$

2) Calculate ID_k by XORing P_2 with hash value of concatenation SN and P_1 :-
$ID_k = P_2 \oplus h\ (SN^e \parallel P_1)$

3) Calculate RM^e by XORing P_3 with UN_u^e :-
$RM^e = P_3 \oplus UN_u^e$

4) Calculate M_{ts}^e by hashing concatenation of values SN^e, RM and UN_u^e :-
$M_{ts}^e = h\ (SN^e \parallel RM^e \parallel N_u^e)$

5) Check whether $M_{ts} = M_{ts}^e$?

6) Generate a random nonce N_j.

7) Calculate X_k^* by hashing concatenation of ID_k and K_s
$X_k^* = h\ (ID_k \parallel K_s)$

8) Calculate M_{sv} by hashing concatenation of values ID_j, N_j, X_k^* and ID_k (Identity of K^{th} user) :-
$M_{sv} = h\ (ID_j \parallel N_j \parallel X_k^* \parallel ID_k)$

9) Calculate D_1 by XORing N_j and hash value of ID_i :-
$D_1 = N_j \oplus h(ID_k)$

10) Calculate D_2 by XORing ID_k and hash value of ID_i :-
$D_2 = ID_j \oplus ID_k$

11) Send M_{sv}, D_1, D_2 via insecure channel to vehicle sensor.

In the sink node, N_u is calculated by XORing SN^e and P_1. In the same way calculate ID_k by XORing P_2 with hash value of concatenation SN and P_1 and then calculate RM^e by XORing P_3 with UN_u^e.Also calculate M_{ts}^e by hashing concatenation of values SN^e, RM and UN_u^e. Now check whether M_{ts}^e generated here is equal to that original message.

If yes, then proceed to the next steps. Generate a random nonce N_j and calculate X_k^* by hashing concatenation of ID_k

and K_s. M_{sv} is calculated by hashing concatenation of values ID_j, N_j, X_k^* and ID_k (Identity of K^{th} user).Calculate D_1 by XORing N_j and hash value of ID_i. Then D_2 is calculated by XORing ID_k and hash value of ID_i. Send M_{sv}, D_1, D_2 via insecure channel to vehicle sensor. With this the authentication phase 1 at the sink node is completed.

D. Authentication Phase- 2 (In vehicle sensor)

The authentication phase 2 takes place at vehicle sensor node. All the authentication requirements at this phase are carefully considered and are met.

1) Calculate N_j^e by XORing hash values of ID_k (given by vehicle sensor) and D_1 :-

$N_j^e = h(ID_k) \oplus D_1$

2) Calculate ID_j by XORing SN^e and P_1 :-

$ID_j = ID_k \oplus D_2$

3) Now the X_k value received from the Registration Authority in response to the ID_k sent to them via the secure channel is used.

4) Calculate M_{sv}^e by hashing concatenation of values ID_j, N_j, X_k and ID_k :-

$M_{sv}^e = h(ID_j \| N_j \| X_k \| ID_k)$

5) Check whether $M_{sv} = M_{sv}^e$?

6) Generate a random nonce N_k.

7) Calculate V by hashing concatenation of ID_k , N_k and N_j :-

$V = h(ID_k \| N_k \| N_j)$

8) Calculate M_{vs} by hashing concatenation of values V, N_j and X_k :-

$M_{vs} = h(V \| N_j \| X_k)$

9) Calculate T_1 by XORing N_j and N_k :-

$T_1 = N_j \oplus N_k$

10) Send M_{vs} and T_1 via insecure channel to sink node.

First of all, in the authentication phase 2 at the vehicle sensor the need is to calculate N_j^e by XORing hash values of ID_k (given by vehicle sensor) and D_1.Then calculate ID_j by XORing SN^e and P_1. Now the X_k value received from the Registration Authority in response to the ID_k sent to them via the secure channel is used. Calculate $M_{sv}^e{}_{by}$ hashing concatenation of values ID_j, N_j, $X_k$and ID_k. Now check whether M_{sv} that is generated is equal to the M_{sv}^e or not.
If yes, then the further process takes place. Generate a random nonce N_k and calculate V by hashing concatenation of ID_k , N_k and N_j. Calculate M_{vs} by hashing concatenation of values V, N_j and X_k.T_1 is calculated by XORing N_j and N_k. Send M_{vs} and T_1 via insecure channel to sink node. With this the authentication phase 2 are vehicle sensor is completed.

E. Authentication Phase- 3 (In Sink Node)

1) Calculate N_k^e by XORing hash values of N_j and D_1 :-

$N_k = N_j \oplus T_1$

2) Calculate V^* by hashing concatenation of N_k, ID_k and N_j :-

$V^* = (ID_k \| N_k \| N_j)$

3) Calculate M_{vs}^ehashing concatenation of values V, N_j and X_k :-

$M_{vs}^e = h(V^* \| N_j \| X_k)$

4) Check whether $M_{vs} = M_{vs}^e$?

5) Calculate W by XORing N_j and N_u :-

$W = N_j \oplus UN_u$

6) Calculate M_{st} by hashing concatenation of values SN^e, N_u, N_j, $HUID_i$ and ID_k :-

$M_{st} = h(SN^e \| UN_u \| N_j \| HUID_i \| ID_k)$

7) Send M_{st} and W via insecure channel to user.

In the authentication phase 3 again at the sink node the need is to calculate N_j^e by XORing hash values of ID_k (given by vehicle sensor) and D_1. Then calculate V^* by hashing concatenation of N_k, ID_k and N_j. M_{vs}^e is to be calculated by hashing concatenation of values V, N_j and X_k. After this check whether M_{vs} is equal to M_{vs}^e or not. If yes , then continue the process. Or else do not continue. Calculate W by XORing N_j and N_u.Calculate M_{st} by hashing concatenation of values SN^e, N_u, N_j, HID_i and ID_k. M_{st} and W that are calculated in these phases are then sent via insecure channel to user.

(At the User)

1) Calculate N_j^e by XORing hash values of W and N_u :-

$N_j^e = N_u \oplus W$

2) Calculate M_{st}^e by hashing concatenation of values SN^e, N_u, N_j^e, HID_i and ID_k :-

$M_{st}^e = h(SN^e \| N_u \| N_j^e \| HID_i \| ID_k)$

3) $M_{st} = M_{st}^e$?

4) If yes, than the session is established.

At the user calculate N_j^e by XORing hash values of W and N_u. Calculate M_{st}^e by hashing concatenation of values SN^e, N_u, N_j^e, HID_i and ID_k.Then finally check whether M_{st} is equal to M_{st}^e or not. If yes, than the session is established.

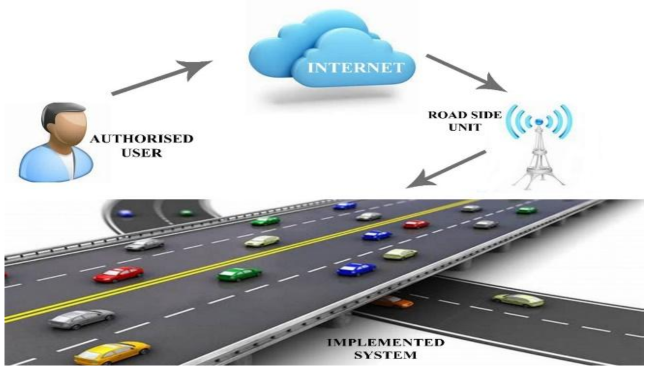

Fig 3 - Schematic Diagram for Smart VANETs

IV. SECURITY ANALYSIS

A detailed analysis of security in the proposed scheme is carried out in this section and thus it has been proven that mutual authentication between units is provided by the proposed protocol. It has also been demonstrated that the security mechanism can resist different attacks such as trace, impersonation, smart card stolen attack, replayattacks, modification attack, man in the middle attack and alteration attacks.

A. Impersonation attack

These attacks are executed by sending the target a message in which the sender attempts to impersonate as a trusted source. This is done in order to gain access to the critical and sensitive information of the target, such as financial data.

If an intruder U_a tries to impersonate as atrue user U_i, U_a must initiate a login request message $\{M_{ts}, P_1, P_2, P_3\}$ successfully. However, U_a is unable to compute these because U_a do not know the actual identity of U_i and its hidden parameters SN, RM and N_u. In addition, U_a does not retrieve a random nonce RN_u. Therefore, our protocol gives immunity towards impersonation attacks because U_a can never produce valid messages.

B. Traceability Attack and Anonymity

In this type of attack, by examining all the inward and outward ports starting from the first host under attack, the intruder tracks the existing attack flow**.** In our protocol, an attacker U_a cannot trace anauthorised user U_i or vehicle. This is because for every session the messages that are transmitted are continuously changed. Also, U_i sends the dynamic identity HUID = h (UID || RN_u), HPWD = h (PWD || RN_u), and RM = h (HUID || HPWD || $RN_{s)}$ to the sink node. To track a true user's work or movement, an attacker must have information about the user's true identity UID, unique password PWD, and nonce RN_u . Because of these reasons, security against traceability attacks and anonymity are provided by this protocol.

C. Smart Access Card Stolen Attack

It is assumed that an adversary U_a can obtain a Smart Access Card (SAC) and extract the parameters {SN, RM, RNs, HNu}. As the parameters that are stored in the smart card are masked as RM = h (HUID || HPWD || RN_s), SN = $h(K_s) \oplus h(HPWD) \oplus h(RN_s)$, HN_u = h (UID || PWD) $\oplus$ RN_u , M_{ts} = h (SN || RM || N_u) by the hash function and XOR operation, the adversary cannot obtain any important information without UID and PWD.

D. Replay Attack

It is assumed that an attacker U_a tries to impersonate as an authentic user U_i by again sending the messages sent in the previously occurred session, U_a cannot mimic U_i successfully. In our proposed protocol, the sink node makes sure that the random nonce is fresh and used previously. The login request is rejected if the random nonce used is not fresh. As $U_a$cannot get random nonce RN,registration message Mts cannot be successfully generated.Thus it couldbe said that the proposed protocol has the immunity to resist itself from all kinds of replay attacks.

E. Man in the Middle Attack

The security analysis that has been done by authenticating the message helps us to infer that the proposed scheme will provide authentication by using the extra variable P_3 for XORing Registration message with random nonce. Therefore, the protocol proposed by us can very well provide security against this kind of attack.

F. Alteration Attack

If an intruder tries to modify the contents present in the network, then it comes under alteration attack. From the algorithm of the protocol, it could be inferred that $\{M_{ts}, P_1, P_2, P_3\}$ is a digital signature. Based on this, any alteration of the message $\{M_{ts}, P_1, P_2, P_3\}$ could be found by ensuring whether the equation $M_{ts} = M_{ts}^{e}$ holds. Therefore, the given scheme prevents these kinds of attacks.

V. AVISPA TOOL VALIDATION

Validation of the protocol that is proposed is done in this section. This validation is done by a widely used and accepted software tool called AVISPA. It stands for "Automatic validation of Internet Security Protocol and Applications".

```
File

role user (U1,S1,V1:agent,
                    SKu1s1: symmetric_key,
                    % H is one−way hash function
                    H: hash_func, SND, RCV: channel(dy))

% Player: the user U1
played_by U1

def=
local State :   nat, UID,PWD,RNu,HUID,HPWD,HNu,IDk,RM,SN,RNs,UNu,Mts,P1,P2,P3,
                    Mst,W,Nj,IDj:text

                    const user_sink,sink_user,sink_vehicle,vehicle_sink,
                    ps1,ps2,ps3,ps4,ps5,ps6 : protocol_id


init State := 0

transition

          % User registration phase
          1. State = 0 ∧ RCV(start) =|>
          % Send the registration request <HUID, HPWD> to Sink Node(S1) securely
          State':=1∧RNu':=new()
          ∧ HUID' := H(UID.RNu')
          ∧ HPWD' := H(PWD.RNu')
          ∧ SND({HUID'.HPWD'}_SKu1s1)
          ∧ secret({HUID',HPWD'}, ps1, {U1,S1})
          ∧ secret({PWD}, ps2, {U1})
          % Receive the smart authentication card <SAC> from Sink Node(S1) securely
```

AVISPA code

```
File

SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/minor.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 0 states
 Reachable  : 0 states
 Translation: 0.29 seconds
 Computation: 0.00 seconds
```

ATSE verification

```
File

% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/minor.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.22s
 visitedNodes: 8 nodes
 depth: 3 plies
```

OFMC verification

VI. PERFORMANCE EVALUATION

Comparison of our protocol's communication and computation costs with other protocols [21, 22, 23 and 24] that are similar to it and discussing theirvarious properties related to security is done in this section.

A. Computation Cost

The overheads of presented protocol have been compared with those of the similar protocols[21, 22, 23 and 24].The following notation has been used to compare the computation cost. T_h, T_a and T_e denotes the usage of hash operation, scalar point operation and curve cryptographic operation respectively

The computation cost of our protocol is $8T_h$ for user, $13T_h$ for sink, $4T_h$ for vehicle sensor. Therefore the entire computation cost for this protocol is $25T_h$ seconds which is quite low.

Schemes	User	Sink Node	Sensor	Total cost
Choi et al. [21]	$12T_h + 3T_e$	$5T_h + T_e$	$7T_h + 2T_e$	$24T_h + 6T_e$
Xue et al. [22]	$10T_h$	$14T_h$	$6T_h$	$30T_h$
Chang et al.[23]	$15T_h$	$18T_h$	$6T_h$	$39T_h$
Kumari and Om[24]	$10T_h$	$8T_h$	$6T_h$	$24T_h$
Ours	$8T_h$	$13T_h$	$4T_h$	$25T_h$

T_h: One-way hash operation, T_a: Symmetric key Cryptographic operation, T_e: Elliptic curve scalar point multiplication operation.

B. Security properties

The protocol proposed by us is capable of resisting various attacks that were possible in other protocols which lack security from various attacks. Considering these things in mind, we can, say that our protocol offers better security.

Security Protocol	Choi et al. [21]	Xue et al. [22]	Chang et al. [23]	Kumari and Om [24]	Ours
Impersonation Attack	Yes	Yes	Yes	No	Yes
Smart Access Card stolen	Yes	Yes	Yes	Yes	Yes
Anonymity	No	No	Yes	No	Yes
Trace Attack	No	No	No	No	Yes

C. Communication Cost

For the analysis of communication cost, we clearly know that operations used in curve cryptographic operation are costlier than hashing operations. Consequently, the total Communication Cost of our proposed scheme is very low than other protocols as they use costly operations. So, our protocol is communication cost efficient.

Search time for our proposed protocol is nearly 0.22 secs which is very less when compared to other protocols which are nearly 0.35 secs. Total parse time is 0.00 secs. A total number of nodes that are visited is equal to 8 which is almost twice to the previous authentication protocols which visit only 4. A depth of 3 piles is obtained by implementing the system with our proposed protocol and the results are very good as the previous protocols reach a depth of only 2 piles.

Translation time of only 0.29 secs is also an added advantage where the other systems have it nearly to 0.45 secs. Computation time is also as low as 0.00 secs.

VII. CONCLUSION AND FUTURE SCOPE

In this research paper, efforts are made to develop a new security mechanism for VANETs in Wireless Sensor Network to overcome the issue of road moving vehicles like relief from traffic congestion and other similar problems. An efficient authentication protocol that is immune from various external attacks has been proposed. The security analysis done on the proposed protocol shows that it has a better performance and enhanced security without increasing the overall cost. Simulation using AVISPA tool has also been done, which shows that attacks like smart card stolen attack and replay attack do not have any impact on our proposed scheme. The protocol proposed by us has its direct application in vehicular system. In the future, the cloud technology and IOT could also be included in order to come out with a more enhanced and practically suitable authentication protocol.

REFERENCES

[1] Hubaux, Jean-Pierre, Srdjan Capkun, and Jun Luo. "The security and privacy of smart vehicles." *IEEE Security & Privacy* 2.3 (2004): 49-55.

[2] Perrig, Adrian, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E. Culler. "SPINS: Security protocols for sensor networks." *Wireless networks* 8, no. 5 (2002): 521-534.

[3] He, Debiao, Sherali Zeadally, Baowen Xu, and Xinyi Huang. "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks." *IEEE Transactions on Information Forensics and Security* 10, no. 12 (2015): 2681-2691.

[4] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, *38*(4), 393-422.

[5] Lewis, Frank L. "Wireless sensor networks." Smart environments: technologies, protocols, and applications (2004): 11-46.

[6] Islam, SK Hafizul, Mohammad S. Obaidat, Pandi Vijayakumar, Enas Abdulhay, Fagen Li, and M. Krishna Chaitanya Reddy. "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs." *Future Generation Computer Systems* 84 (2018): 216-227.

[7] Chandrakar, P., & Om, H., "A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC," Computer Communications, vol. 110, pp. 26-34, 2017.

[8] Chandrakar, P., & Om, H., "Cryptanalysis and extended three-factor remote user authentication scheme in multi-server environment", Arabian Journal for Science and Engineering, vol. 42(2), pp. 765-786, 2017.

[9] Ali R, Pal AK, Kumari S, Karuppiah M, Conti M., "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring", Futur Gener Comput Syst. https://doi.org/10.1016/j.future.2017.06.018.

[10] Chandrakar, P., & Om, H., "Cryptanalysis and improvement of a biometric- based remote user authentication protocol usable in a multiserver environment", Transactions on Emerging Telecommunications Technologies, vol. 28(12), e3200, 2017.

[11] Chandrakar, P. and Om, H., "An extended ECC- based anonymity- preserving 3- factor remote authentication scheme usable in TMIS", International Journal of Communication Systems, vol. 31(8), p.e3540, 2018.

[12] Chandrakar, P., "A Secure Remote User Authentication Protocol for Healthcare Monitoring Using Wireless Medical Sensor Networks", International Journal of Ambient Computing and Intelligence (IJACI), vol. 10(1), pp.96-116, 2019.

[13] Chandrakar, P. and Om, H., "An efficient two-factor remote user authentication and session key agreement scheme using rabin cryptosystem", Arabian Journal for Science and Engineering, vol. 43(2), pp.661-673, 2018.

[14] Ali, R. and Pal, A.K., "Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment", Arabian Journal for Science and Engineering, vol. 42(8), pp.3655-3672, 2017.

[15] Chandrakar, P. and Om, H., "Cryptanalysis and security enhancement of three-factor remote user authentication scheme for multi-server environment. International Journal of Business Data Communications and Networking (IJBDCN), vol. 13(1), pp.85-101, 2017.

[16] Chandrakar, P. and Om, H., "RSA based two-factor remote user authentication scheme with user anonymity", Procedia Computer Science, vol. 70, pp.318-324, 2015.

[17] Chandrakar, P. and Om, H., 2017, March. A Secure and Privacy Preserving Remote User Authentication Protocol for Internet of Things Environment. In International Conference on Computational Intelligence, Communications, and Business Analytics (pp. 537-551). Springer, Singapore.

[18] Ali, R. and Pal, A.K., "An efficient three factor–based authentication scheme in multiserver environment using ECC", International Journal of Communication Systems, vol. 31(4), p.e3484, 2018.

[19] Chandrakar, P. and Om, H., 2015, November. A secure two-factor mutual authentication and session key agreement protocol using Elliptic curve cryptography. In Computer Graphics, Vision and Information Security (CGVIS), 2015 IEEE International Conference on (pp. 175-180). IEEE.

[20] Ali, R. and Pal, A.K., "A secure and robust three-factor based authentication scheme using RSA cryptosystem", Int J Bus Data Commun Netw, vol. 13(1), pp.74–84,2017.

[21] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, Security enhanced user authenti-cation protocol for wireless sensor networks using elliptic curves cryptography, Sensors 14(6) (2014) 10081–10106.

[22] K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentica-tion and key agreement scheme for wireless sensor networks, J. Netw. Comput. Appl. 36(1) (2013) 316–323.

[23] C.-C. Chang, W.-Y. Hsueh, T.-F. Cheng, A dynamic user authentication and key agreement scheme for heterogeneous wireless sensor networks, Wirel. Pers. Commun. (2016) 1–19.

[24] Kumari, Shipra, and Hari Om. "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines." *Computer Networks* 104 (2016): 137-154.

[25] Toh, C. K. (2002). Ad hoc mobile wireless networks: protocols and systems (Vol. 11104). Springer.

[26] Mohit, Prerna & Amin, Ruhul & Biswas, G.P.. (2017). Design of authentication protocol for wireless sensor network-based smart vehicular system. Vehicular Communications. 9. 10.1016/j.vehcom.2017.02.006.