I J C T A, 9(37) 2016, pp. 1015-1025

Review and Analysis of Session Initiation Protocol using ECC in VANET

Hari Krishna[1], Sandeep Kumar Arora[2] and Gurjot Singh Gaba[3*]

ABSTRACT

Vehicular Ad-hoc network (VANET) is a wireless communication among many vehicles. The main motive of VANET security is not only to provide safety, secure communication and intelligent transportation service but also another services like entertainment, advertisement and offers based on location. Security is one of the major concern in VANET since various nodes in VANET are mobile in nature. So this is a challenging work to design an efficient solution for secure communication in VANET since nodes are highly mobile. In this paper, we have reviewed and analyzed the impact of the stolen verifier attack and user anonymity attack on various Quality of Services (QoS) in different traffic scenarios. We also proved that after applying Elliptic Curve Cryptography(ECC) there is an improvement over QoS.

Keywords: VANET, Quality of Services, Session Initiation protocol, ECC, VoIP, V2V, V2I

I. INTRODUCTION

Modernization and technological advancement leads to increase in traffic which leads to various road accidents in absence of road safety. In addition, there is wastage of energy and resources and increase in pollution. As all the services related to communication are more important and vulnerable to attacks hence requires security. In VANET, vehicles represent the node and communication taking place either between Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I). Securing communications between vehicles and road side unit is a great challenge. In literature, there are various protocols for authentication have been suggested for secure communication in VANET using Session Initiation Protocol (SIP). SIP basically focus on signaling, and creating communication among dissimilar nodes in VANET. Voice over Internet Protocol (VoIP) concept is used in SIP for communication among cars. It uses HTTP (Hypertext Transfer Protocol) digest for identity authentication between different vehicles during communication. In this paper, a SIP authentication protocol for various vehicles is proposed to address these issues. The security system of proposed scheme [1] is more secure with respect to different types of attacks. The effectiveness of the proposed scheme confirmed by safety.

HTTP verification system [3] is first authentication for Session Initiation Protocol(SIP). It is analysed by Yang et al. [5] that vulnerable attack and off-line password predicting attack is the main problem in HTTP digest. Further Yang et al. [5] tried to add more security in previous scheme and given a new secured scheme. But Huang et al. [4] indicated that those users who have limited computational power, Yang et al. [5] scheme is not appropriate and has given a useful authentication algorithm for session initiation protocol(SIP). Later on weaknesses like off-line password predicting attack found in both Huang et al. as well as Yang et al. and it is demonstrated by Jo et al. [6]. Taking reference of Yang et al. work SIP-ECC, a new authentication technique is suggested by Duralink and Sogukpinar [8]. Miller [7] and Koblitz [9] first introduced ECC separately. ECC uses a smaller key size with respect to the traditional public key

[1,2,3] Discipline of Electronics and Communication Engineering, Lovely Professional University, Phagwara, Punjab, India - 144411, *E-mails:* [1]*hrkrishna116@gmail.com,* [2]*sandeep.16930@lpu.co.in,* [3]*er.gurjotgaba@gmail.com*[*]

[*]*Corresponding Author*

Cryptography and provide the same security. So we can say Performance wise Duralink and Sogukpinar. But there is two vulnerability Denning-Sacco and the off-line password predicting attack still present in Duralink and Sogukpinar and these attacks were find out by Yoon and Yoo [10] and they suggested a new enhanced scheme to countermeasure this problem. Later on, Liu and Koenig [11] found that there are still two vulnerabilities the insider attack and the password guessing attack present in Yoon and Yoo's scheme.

To improve safety and performance, Tsai [12] used one-way hash function and exclusive-or operations for SIP and proposed an effective authentication scheme. But, the stolen-verifier attacks, off-line password predicting and the Denning-Sacco attack is not withstanding by Tsai's scheme [2, 13, 14]. An effective verification arrangement for SIP, is provided by Arshad and Ikram [2] using ECC. There are some weaknesses like off-line password predicting attack in Arshad and Ikram scheme and it is given by Tang and Liu [15]. Yoon and Yoo [14] has given a new scheme [12] using Elliptic curve cryptography for the SIP. But Xie [16] indicated that there is vulnerability of stolen verifier attack and the off-line password predicting attack in Yoon and Yoo's scheme. To overcome these vulnerabilities in Yoon and Yoo's scheme Xie proposed new authentication algorithm for SIP using ECC. After some time, off-line password guessing and Impersation attack found in Xie's scheme by Farah and Attari [17]. Farah and Attari also given an enhanced scheme to countermeasure Xie's scheme. Later on, Zhang, Qi, Neeraj, Chilamkurti and Jeong [1] given a scheme which can not only withstand user anonymity attack but also replay attack, password guessing attack, man-in-the-middle attack, Denning-Sacco attack, stolen-verifier attack. In this paper, we have taken reference of Zhang and Qi's user anonymity and stolen verifier attack and realized these attacks in different traffic condition and find out the various QoS parameters. Detailed QoS parameter and their graphical analysis is presented in further section. The paper description and organization are as follows

II. SIP-ECC AUTHENTICATION SCHEME

In this part, we have used the Zhang and Qi's [1] proposed algorithm for authentication with user anonymity for the SIP using the elliptic curve cryptography. SIP-ECC scheme includes four phases first system arrangement phase, second registration phase, third login and authentication phase, and finally password change phase.

(A) System Setup Phase

In this phase, the server S generates the system parameters through the following steps.

- q is generated by S. E(GF(q)) represents an elliptic curve over the Galois finite field GF(q) and point P represents the generator of the additive group E(GF(q)).
- A long-live secret key randomly $ks \in Z^*q$ is generated by S and long live public key Qs=ks.P is also computed by the S.
- first a secure hash function $h(\cdot)$ is selected by S then he/she publish the system parameter like {q, E(GF(q)), P, h (·), Qs}.

(B) Registration Phase

To access the remote server S services, first user U have to register to S and then follow these steps.

- U is allowed to freely select username and password PW of his choice. Afterwards he has to send the username and password to remote server S via secure medium. We use secure sockets layer protocol to implement the secure medium.
- S have to compute the verifier password VPW= h(username||ks)⊕h(username||PW) after receiving username and PW and store (username,VPW) in to their database.

(C) Login and Authentication Phase

To access the server S services remotely, user U go through following algorithm. First user U and server S will authenticate each other using following steps.

- A random number a∈Z*q is generated by user U and then computes A=aP, Tu = aQs, $\overline{username}$ = *username* ⊕h (A||Tu), and sends REQUEST{ $\overline{username}$,A} as the request message to S.
- S generates a random number b∈Z*q, after receiving the message REQUEST{ $\overline{username}$,aP} and then computes B=bP, Ts=ksA, SKs=baP and α=h(Ts||SKs||B||A). Then, S sends CHALLENGE{realm, B, α}as the challenge message to U.
- U computes SKu=abP, after receiving the CHALLENGE{realm,B,α} message, and checks whether the equation α=h(Tu||SKu||B||A) is valid or not. If α validity then session is stopped by user U; otherwise a session key SK=h(username||SKu||Tu||A||B),β=h(realm||Tu||SKu||B||A||h(username||PW)) is generated by user U and then send RESPONSE{realm,β}as the response message to S.
- After receiving RESPONSE{realm, β} message, S computes username = $\overline{username}$ ⊕h (A||Ts) and check for the validity of β whether the equation β = h(realm||Ts||SKs||B||A||h(username||PW)) valid or not, where PW′ =VPW⊕h(username||ks). If β is not valid then session is stopped by S; otherwise, S continue to compute session key SK= h(username||SKs||Ts||A||B).

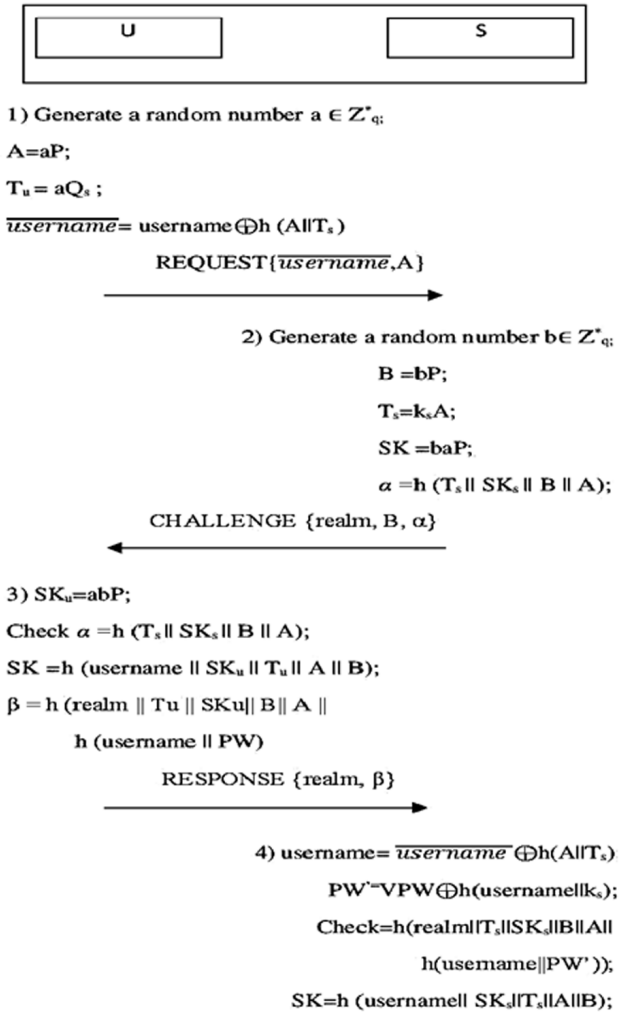

Figure 1: Login and authentication algorithm [1]

(D) Phase of password change

In this stage user U will modify his/her password with the assistance of the distant server S. For security reason, U and S generate a session key SK after implementation of the login and verification phase. Detail explanation are as follows:

- First user U will select a new password PW^{new}, and calculate $\sigma = h$ (username ||SK||h (username||PW)||h (username||PWnew)),PWD=h(SK||h(username||PW))⊕h(username||PW^{new}), then send message {username, σ, PWD} to S.
- S receive {username, σ, PWD} as the message and tries to find out h(username||PW^{new})= PWD⊕h(SK||h(username||PW′)) and verify whether the equation σ = h(username|| SK||h (username||PW2)||h(username||PW^{new})) is correct, where PW =VPW ⊕ h(username||ks). If the equation is wrong then session is stopped by S; otherwise, S replace VPW with VPW^{new}=h(username||ks)⊕h(username||PW^{new}).

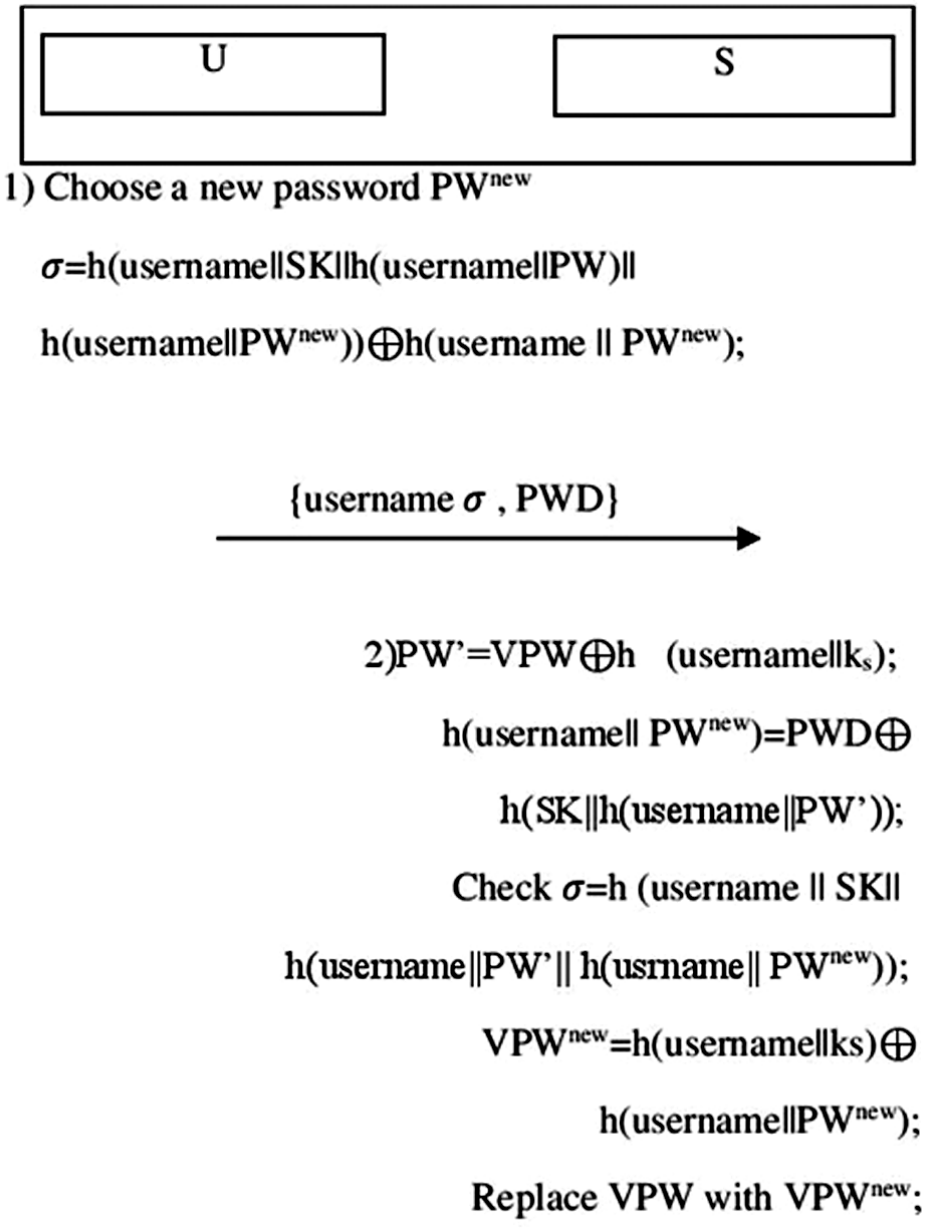

Figure 2: Algorithm for password change phase [1]

III. AUTHENTICATION SCHEME FOR USER ANONYMITY

We are working to make a multifaceted topology with more no. of nodes. In this, the mobility is given to all nodes with different timings. Hence nodes will be in mobile at the respective time. Here we are using AODV protocol and we will be routed using the same. User anonymity attack will be introduced in the network to check the performance. We will take values of QOS parameters like end to end delay, energy spent, packet delivery ratio, throughput at the corresponding time like 2, 4,6,8,10 ms. We will insert the values in a scheme produced trace file and graph will be plotted for each parameter.

User anonymity means during the login and authentication phase the attacker try to get identity of the user from transmitted message. In this scheme, the protected $\overline{username}$ send as identity in place of username, the user sends to the server, where $\overline{username}$ = username $\oplus$h (A||T_u), A=aP and T_u=ak_sP. The attacker has to compute ak_sP from A=aP and Q_s=k_sP. Attacker has to compute Diffie-Hellman problem if he tries to get the identity of user. Hence, this scheme [1] for SIP provide better authentication for user anonymity.

IV. AUTHENTICATION SCHEME FOR STOLEN VERIFIER ATTACK

In this configuration, the mobility values are provided to all nodes with different timings. Hence nodes will be in mobile using AODV at the respective time. Stolen verifier attack will be introduced in the network to check the performance. We will take values of QOS parameters like end to end delay, energy spent, packet delivery ratio, throughput at the corresponding time like 2, 4,6,8,10 ms. We will insert the values in a system generated trace file and graph is plotted for each parameter.

In case of stolen-verifier attack, attacker tries to login in the remote server, for that he/she tries to steal the verifier password already stored in the remote server's database. Remote server stores (username, VPW) at the time of proposed scheme registration phase, where VPW= h(username||ks)$\oplus$h(username||PW). The attacker could steal (username, VPW). But attacker is not able to get the verifier password h(username||PW) because they don't know the secret key ks of server. Hence, we can say that this authentication scheme [1] for SIP prevents the stolen verifier attack.

V. RESULTS AND ANALYSIS

(A) Generation of Traffic with respect to Number of Nodes

We are going to build a wireless ad-hoc network to transmit the packets. Building a simple topology with different traffic scenarios for e.g. 10,30 and 50 nodes for low, medium and high traffic respectively will be deployed in the network.

Table I
Simulation Parameter

Simulation Parameters	*Values*
Number of nodes	10, 30, 50
Propagation model	Two ray ground
Antenna type	Omni directional
Routing protocol	AODV
MAC	802.11
Packet size	200
Simulation area	500*500

We are using AODV routing protocol for packet transmission. Considering that at the start of the communication there is no attack.

After analysing above algorithm in different traffic scenario we found the following results. Moreover, we have analysed all three-traffic conditions and given the graphical representation. In this paper, for graphical representation we have only shown the low and high traffic but we have given the comparative results in tabular form for effective analysis.

(B) Comparative Geographical Analysis of QoS in Low and High Traffic Scenario

We are considering the low traffic in which only 10-nodes and high traffic scenarios in only 50-nodes are communicating among themselves. Nodes are transmitting their data to interested user using Ad-hoc On-Demand Distance Vector protocol (AODV). In these traffic scenarios, we have also considered that attacker node also mixed with nodes and try to access the data transmitted in the network. Here we are considering only user anonymity attack and stolen verifier attack. To save the node's session from user anonymity attack and stolen verifier attack we are using Elliptic Curve Cryptography(ECC) and comparing the QoS like delay, energy, throughput and packet delivery ratio.

1) Average Delay in Low and High Traffic: Initially average delay of nodes less when simple AODV protocol is implemented. When network is deployed, and considering no attack then in case of AODV delay is 2.49% more in high traffic. As time passes attackers are activated in the communication. Packet loss in the network creates the delay and it is 50.52% more in high traffic for user anonymity and in stolen verifier attack average delay is approximately 50.73% with respect to low traffic. When ECC is implemented, the session become secure now to access the data the attacker has to face computational Diffie-Hellman problem so there will be no packet loss hence the average delay is very less in case of ECC.

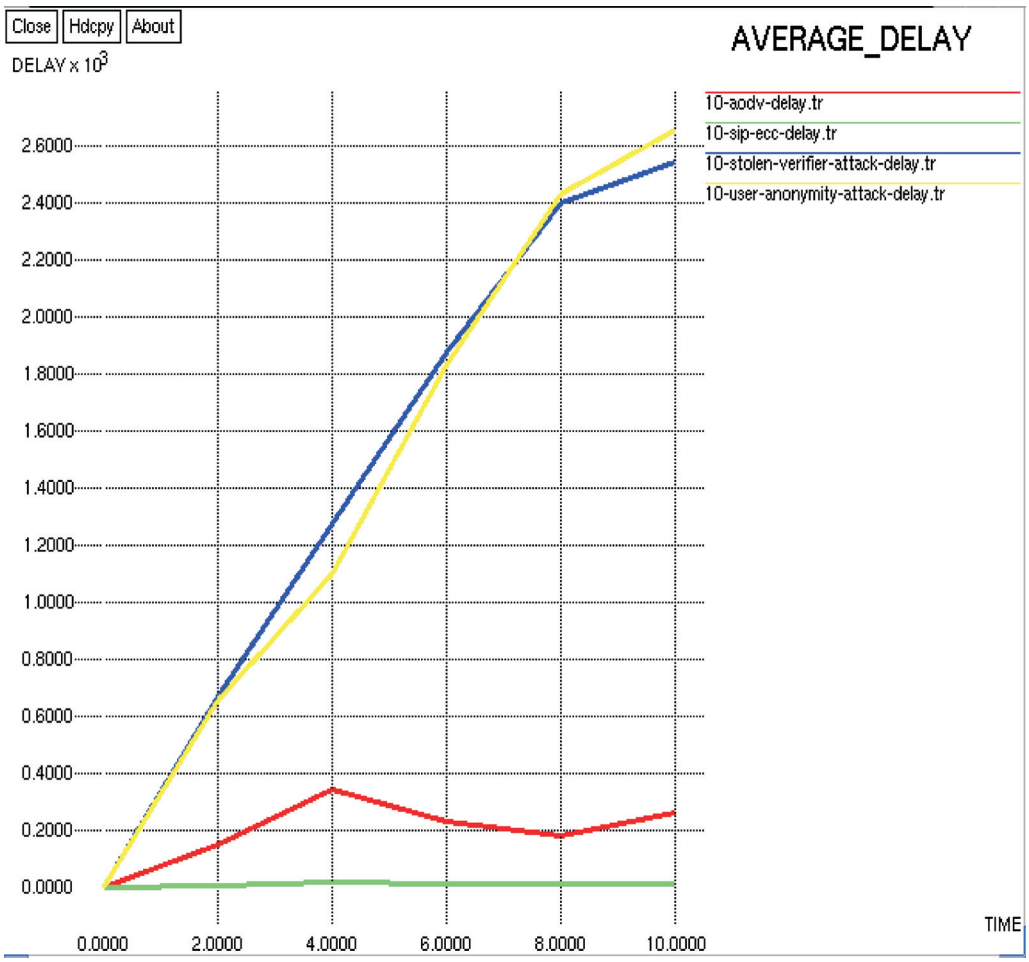

Figure 1: Comparison of Average Delay(10-nodes)

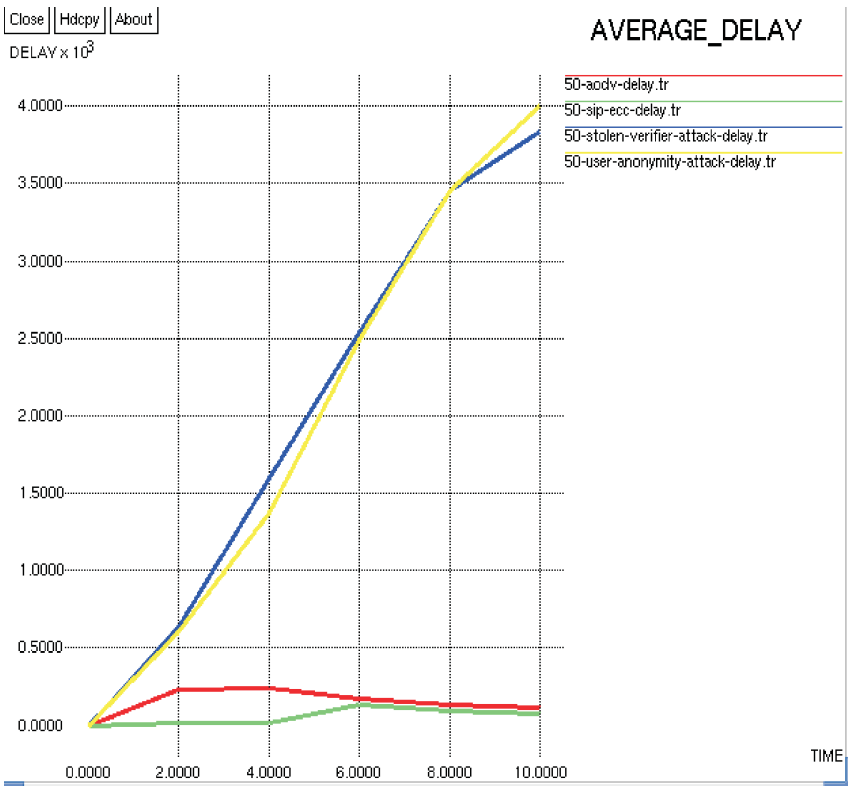

Figure 2: Comparison of Average Delay(50-nodes)

2) Energy in case of low and high traffic: The energy of the nodes in high traffic when compare to low traffic is 12.82% in user anonymity and it is 12.85% in case of stolen more due to loss of packets but in AODV it is lesser approximately 5.91%. Energy of user anonymity and stolen verifier are almost same so plots are overlapping. When we apply ECC technique to make communication secure so there will be no packet loss hence the energy required is decreased to 77.41%.

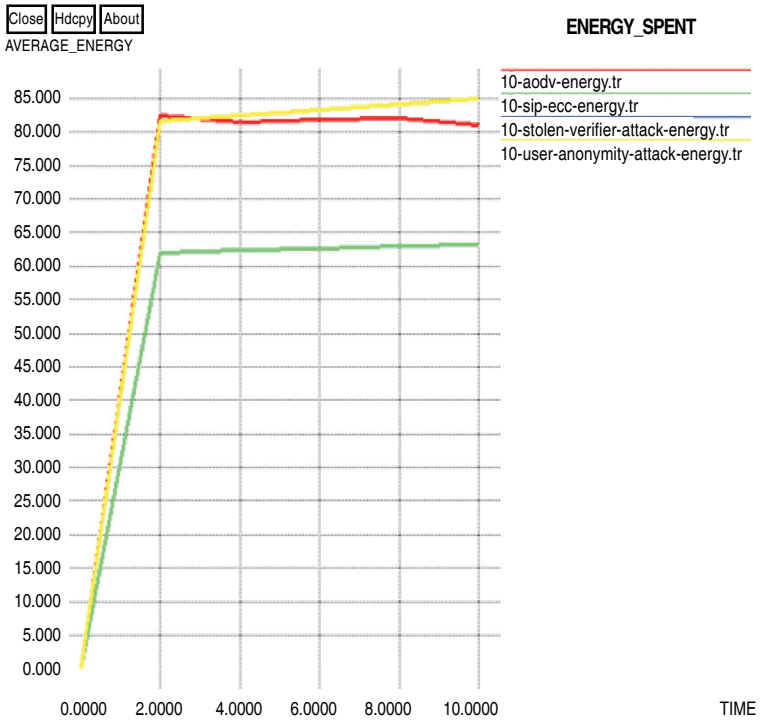

Figure 3: Comparison of Energy Spent (10-nodes)

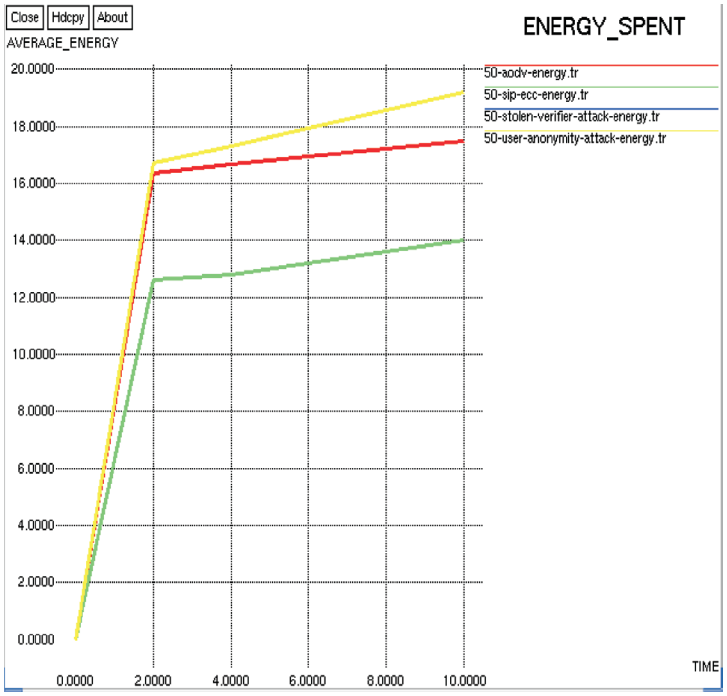

Figure 4: Comparison of Energy Sprnt(50-nodes)

3) Average Delay in Low and High Traffic: In case of low traffic, the average throughput of the various nodes is shown in the Fig. 7. When nodes are in communication using AODV protocol the throughput is initially increasing and after that slightly starts decreasing as time increases. It is because of bit error rate increase as time passes. For user anonymity attacks, in high traffic with respect to low traffic, throughput is 17.40 % less and in stolen verifier attack it is 2.77% less. When we implemented ECC throughput is approximately 42% improved as we can see in the Fig. 8.

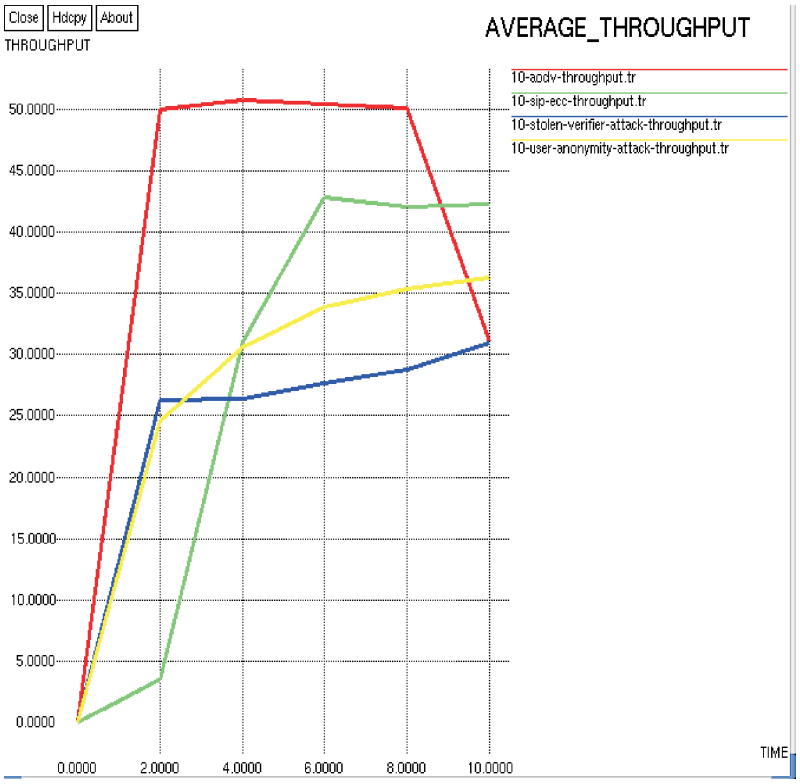

Figure 5: Comparison of Average Throughput(10-nodes)

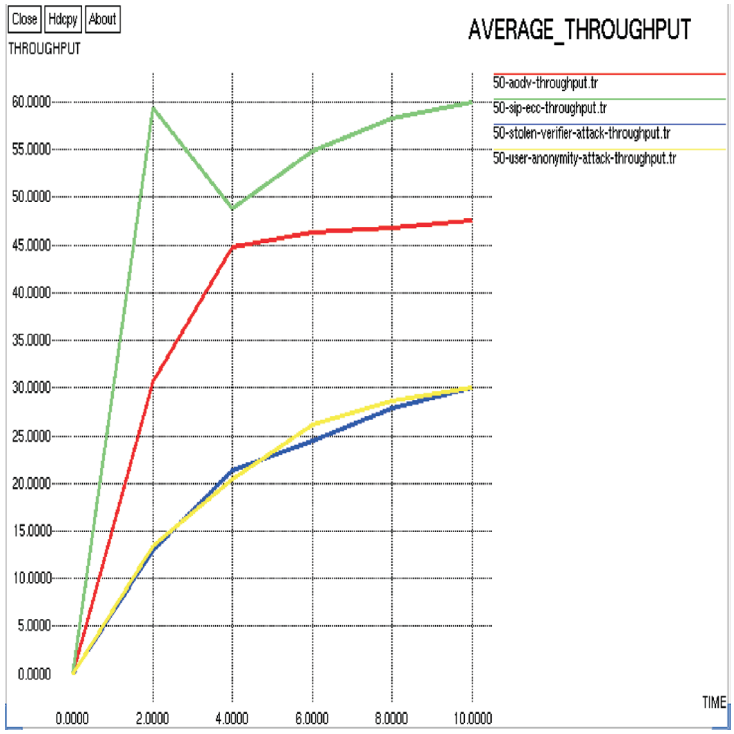

Figure 6: Comparison of Average Throughput(50-nodes)

4) Packet Delivery Ratio (PDR) in Low and High Traffic: The packet delivery ratio in both low and high traffic is shown in Fig. 9, by observing the graph, we can say that as time passes the PDR is increased to 10.96% in case of AODV as there are more node. In case of high traffic with respect to low traffic for user anonymity PDR is decreased by 27.48% and in case of stolen verifier attack it is decreased by 83.68% since most of data traffic is created by attacker so there is a loss of packets but when ECC is implemented PDR is 31.30% less in high traffic w.r.t low traffic because as traffic increases packet loss occurs but it will be less when compare to attacks. So we can say that PDR is improved in comparison to attack up to some extent as shown in Fig.10.

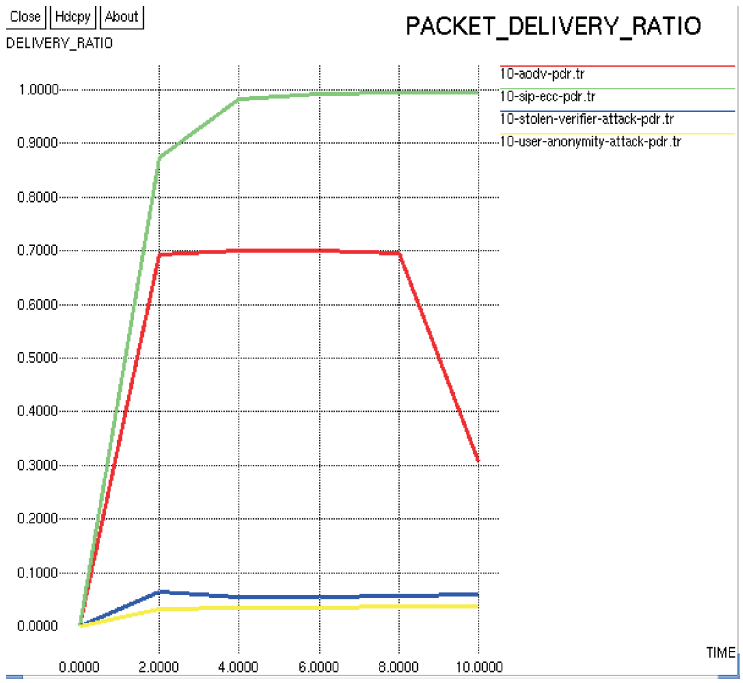

Figure 7: Comparison of Packet Delivery Ratio(10-nodes)

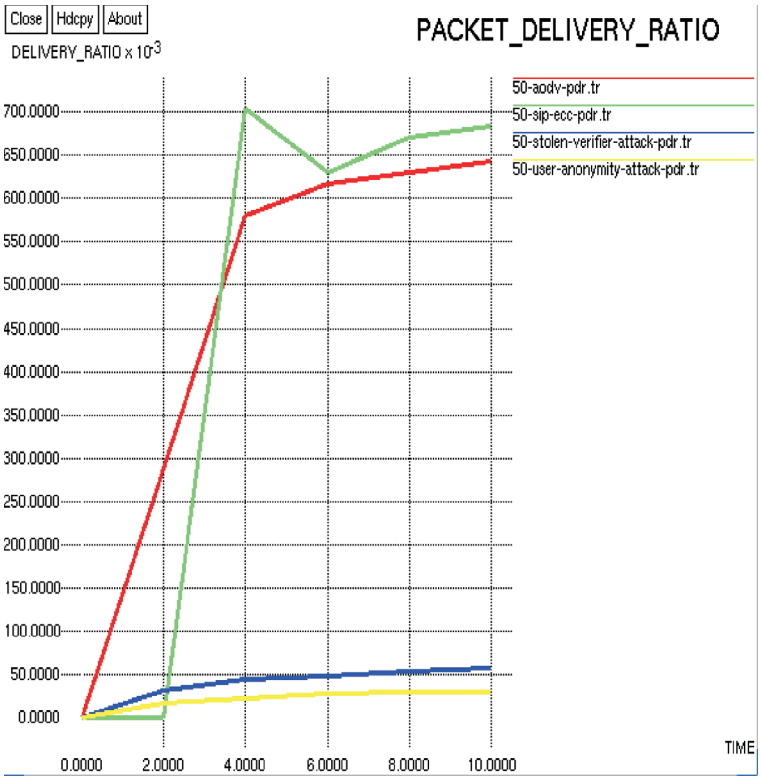

Figure 8: Comparison of Packet Delivery Ratio(50-nodes)

VI. DETAILED COMPARISON OF QOS IN DIFFERENT TRAFFIC PATTERNS

Comparison of all QoS parameters has been shown below in Table II to Table V.

Table II
Comparison of QoS in case of AODV

Traffic Scenario	*Average Delay (ms)*	*Energy (Joule)*	*Average Throughput (Kbps)*	*Packet Delivery Ratio*
Low(10-nodes)	232.87	818.67	46.57	0.6196
Medium(30-nodes)	595.31	829.94	37.26	0.482
High(50-nodes)	177.50	847.03	43.10	0.5518

Table III
Comparison of QoS in case of User Anonymity

Traffic Scenario	*Average Delay (ms)*	*Energy (Joule)*	*Average Throughput (Kbps)*	*Packet Delivery Ratio*
Low(10-nodes)	1735.35	833.5674	32.176	0.0347
Medium(30-nodes)	2450.62	866.68	31.75	0.0343
High(50-nodes)	2385.26	897.56	23.744	0.0253

Table IV
Comparison of QoS in case of Stolen Verifier

Traffic Scenario	*Average Delay (ms)*	*Energy (Joule)*	*Average Throughput (Kbps)*	*Packet Delivery Ratio*
Low (10-nodes)	1752.03	833.80	28.01	0.2905
Medium (30-nodes)	2397.09	886.87	30.75	0.0631
High (50-nodes)	2412.74	897.72	23.35	0.0474

Table V
Comparison of QoS in case of SIP-ECC

Traffic Scenario	*Average Delay (ms)*	*Energy (Joule)*	*Average Throughput (Kbps)*	*Packet Delivery Ratio*
Low (10-nodes)	9.93	62.63	31.98	0.9681
Medium (30-nodes)	8.49	17.61	26.04	0.5677
High (50-nodes)	22.63	10.40	22.89	0.5375

VII. CONCLUSION

In this paper, we have analysed the verification scheme with user anonymity and stolen verifier attack for the SIP using the ECC is implemented and then security analysis shows that scheme not only is secure against common attack such as stolen-verifier attack, but also provides protection against user anonymity. In the used scheme, we have found that time delay is less 97.3 % delivery, energy required is comparatively reduced to 83.39%, throughput is 90 % and packet delivery ratio is also improved i.e. 44.47% so we can say that scheme is better in different traffic scenarios. In future, we can compare various type of cryptographic techniques with ECC to achieve more secure and efficient network communication.

REFERENCES

[1] Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurti, H-Y. Jeong , "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography," ©Springer Science Business Media New York , pp.3477-3488,2014.

[2] R Arshad N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," Multimed Tools Application, vol.66,no.2, pp.165–178,2013.

[3] J. Franks , P.H. Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, "HTTP authentication: basic and digest access authentication," IETF RFC2617, June, 1999

[4] HF. Huang, WC. Wei, GE. Brown, "A new efficient authentication scheme for session initiation protocol," 9th Joint Conference on Information Sciences, 2006.

[5] CC. Yang, RC. Wang, WT. Liu, "Secure authentication scheme for session initiation protocol," computers and Security vol. 24, no.5, pp.381–386, 2005.

[6] H. Jo, Y. Lee, M. Kim, S. Kim, D. Won , "Off-line password-guessing attack to Yang's and Huang's authentication schemes for session initiation protocol," Fifth International Joint Conference on INC, IMS and IDCpp. 618–621, 2009.

[7] VS. Miller, "Use of elliptic curves in cryptography," Advances in cryptology, proceedings of CRYPTO'85, vol. 218. LNCS, Springer-Verlag, pp. 417–26, 1986.

[8] A Durlanik, I. Sogukpinar, "SIP authentication scheme using ECDH," World Enformatika Soc Trans Eng Computer Technology, vol. 8, pp.350–353, 2005.

[9] N Koblitz, "Elliptic curve cryptosystem," Math compute, vol. 48, pp.203–209, 1987.

[10] EJ Yoon, KY. Yoo, "Cryptanalysis of DS-SIP authentication scheme using ECDH," International Conference on New Trends in Information and Service Science**,** pp. 642–647, 2009.

[11] FW. Liu, H. Koenig, **"**Cryptanalysis of a SIP authentication scheme,"12th IFIP TC6/TC11 International Conference, CMS 2011, Lecture Notes in Computer Science, Vol. 7025, pp.134–143, 2011.

[12] JL. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," Internationals Journal Network Security, vol. 8, no. 3, pp.312–316, 2009.

[13] TH. Chen, HL. Yeh, PC. Liu, HC. Hsiang, WK. Shih, "A secured authentication protocol for SIP using elliptic curves cryptography," FGCN 2010, Part I, Communications in Computer and Information Science, Vol. 119, pp. 46–55, 2010.

[14] EJ. Yoon, KY. Yoo, "A new authentication scheme for session initiation protocol," International Conference on Complex, Intelligent and Soft-ware Intensive Systems, CISIS'09. Fukuoka, Japan, pp. 549–554., 2009.

[15] H. Tang, X. Liu, "Cryptanalysis of Arshad et.al ECC-based mutual authentication scheme for session initiation protocol," Multimedia Tools Application, vol. 65 no. 3, pp.165–178, 2013.

[16] Q Xie, "A new authenticated key agreement for session initiation protocol," International Journal Communication System, vol. 25 no.1, pp.47–54, 2012.

[17] MS. Farash, MA. Attari, "An enhanced authenticated key agreement for session initiation protocol.," Information Technology Control, vol. 42, no.4, pp.333–342, 2013.