Security in Third Party Intervened Vertical Handover in Heterogeneous Networks

S. B. Kumbalavati
Department of Electronics and Communication Engineering, Jain University, Karnataka, India
Email:sbkumbalavati@gmail.com

J. D. Mallapur
Department of Electronics and Communication Engineering,
Basaveshwar Engineering College, Bagalkot
Email: bdmallapur@yahoo.co.in

***Abstract*— The present world is encouraging interconnection of different types of networks intern the internet usage for all purpose applications. This leads to ensure seamless handover and repetitive vertical handovers. The heterogeneous network has handover challenge as well as the network security. In our previous work we have proposed third party Intervention for vertical handover. In this proposed work we have extended the previous work by providing security enhancement. The simulation results show that there is a reduction in leakages and attacks after applying our scheme.**

Keyword- Security, Handover, Heterogeneous Networks, UNI_MOB.

I. Introduction

Seamless mobility and roaming is the essential feature of today's wireless communication system. In country like India there is huge demand for seamless internet service access which cannot be met by single operator or single technology. Handover is the important step for this continuous connectivity. It enables the user to maintain session from different access network.

The mobile internet availability made people to access internet any time anywhere. The success of telecom operator lies in providing any time access without affecting the Quality of Service. This requires seamless handover across different networks.

With less availability of spectrum in competitive market like India, to achieve seamless handover, third party handover is needed. The third party handover will brokerage across different operator networks and services to achieve seamless handover. In our earlier work [1], we have proposed the solution for seamless handover using third party handover solution. The third party handover was using Service Oriented Architecture (SOA). The individual operator services integrated with third party server just like accessing a web service with loose coupling and third party server made critical decisions regarding handover and authentication.

The solution was named UNI-MOB in [1] paper. It was to enable SOA based third party vertical handover solution with user centric. But the solution has several security problems and if not addressed attacker can make the solution not-usable. In this paper we survey the different security solutions in vertical handover and list the security problems in our solution and also propose a solution for the security problems without affecting the delay in bigger way. The ultimate aim of the security solution is that light weight without affecting the delay.

The rest of this paper organized as follows. In section 2, we did the literature survey on security in vertical handover. In section 3, defines the problem definition of our proposed work. Section 4 describes the mathematical model for our proposed work. In section 5 analysis the performance of our proposed work via simulations and section 5 concludes this paper.

II. SURVEY

In [2], proposed a Media Independent Pre-Authentication handover optimization framework. It provide optimization for inter domain and inter technology handover, and also achieve significant reduction in handover delay for both network and application layer. In [3], a modified version of Kerberos featuring of sequence-number based service ticket distribution and challenge-response based service access authentication is proposed. It performs Kerberos authentication without relying on time synchronization, which makes authentication between MN and IS more freely. But transport of context multiple times during continuous handover is very time consuming in this process and have to wait for Kerberos setup time.

In [4] authors developed two protocols for authentication and authorization of mobile nodes. Protocol for carrying Authentication for Network Access (PANA) and Extensible Authentication Protocol (EAP) were deployed on IETF architecture to optimize reduction in authentication and authorization latency. In [5] a light weight solution for authentication for seamless handoff was proposed, but the work focused more only privacy preservation and wanted to preserve user anonymity during handover by creating new contexts, but in our solution, we don’t want anonymity as UNI-MOB solution cannot bill customers if anonymity is maintained.

In [6] analysis of two IEFT protocols for vertical handover CAPWAP and HOKEY is analyzed. HOKEY solution for seam less handover is based on establishing key hierarchies and using it for secure context transfer, however this solution is very cumbersome and not light weight. In [7], author proposed a global authentication protocol in 4G networks. This protocol enables a vertical handover without requiring a prior subscription to the visited network. By using this protocol good security level is achieved without introducing complexity and overhead.

In [8], a new authentication mechanism for seamless handover between 802.16e and 3G wireless networks are proposed. According this solution Inter Base Station Protocol (IBSP) message can be transmitted between two heterogeneous networks. Authentication is performed only at initial stage of connecting the user terminal without reauthentication. This approach is good for reducing authentication delay in handover latency but the replay attack can be launched and it can go undetected in the network. In [9] the proposed work presents a multicriteria handoff protocol. This protocol includes the mobility and QoS parameters to trigger handoff. By using evolution prediction model it avoids the pingpong effect in heterogeneous networks.

In [10] proposed an AKA protocol for an open access architecture. The AKA protocol was verified by formal methods and Casper/FDR tool and these methods have proved that AKA protocol provide the security in vertical handover. In [11] author proposed seamless handover mechanism between Wi-Fi and Wi-Max networks to reduce authentication process. This mechanism also involves security that guarantee the handover message to be secure. In [12] proposed a new seamless vertical handover scheme to perform fast authentication while guaranteeing the QoS and security to real time communications. This scheme shows better performance in terms of signaling cost and packet loss for the same.

In [13] author proposed a broker based architecture for integrated heterogeneous networks and extended handover keying protocol to reduce the user authentication delay. This proposed architecture and protocol lead to significant reduction in Vertical Hand Off (VHO) delay, VHO interruption probability and power consumption. In [14] author proposed two discard information policies for Chipper based Message Authentication Code (CMAC). These policies are Shared Authentication Information (SAI) and Shared Authentication Key (SAK). SAI is vulnerable to DDoS attacks and SAK is reducing the latency for authentication during vertical handover.

III.PROBLEM DEFINITION

In our previous work we had proposed a scheme for third party intervened handover called as UNI-MOB, but it was not secured by the attacks, leakage the register context of UNIMOB and the deficiency in continuous authentication. In present work we have extended these security issues.

The security issues in UNI-MOB are

- Replay attack by capturing attach message from UE and forging it to login from some other network.
- Register context kept at UNI-MOB can be leaked.
- There is no continuous authentication

A. Replay Attack

Replay attacks can be launched by capturing the attach message with encrypted token and using it to generate fake attach. So there must be a mechanism in UNI-MOB to authenticate the attach message with less time so it does not affect the handover latency. To achieve this, the encrypted token in attach message is sent to UNI-MOB, it must be able to deduce from the registration context information, what is next expected token and must compare to the encrypted token received now in the attach message and reply pass if both are same or fail if it is different. To reduce the authentication delay, the next expected encrypted token is generated well ahead and kept in registration context at the UNI-MOB platform.

From the initial token, a secure Hash Function H is applied to generate the next token and it is encrypted with the user’s key and stored as next expected token.

$H(token) \rightarrow (tk_1) \rightarrow E(tk_1)$

$H(tk_1) \rightarrow (tk_2) \rightarrow E(tk_2)$

$H(tk_2) \rightarrow (tk_3) \rightarrow E(tk_3)$

…..

$H(tk_n) \rightarrow (tk_n) \rightarrow E(tk_n)$

The hash function is specific for the user and it is generated newly when every time user registers. The hash function is created secure so that subsequent keys can be generated but the previous cannot be deduced. Hash function is replaced for every new session, so even if attacker captures the hash function it is not useful for the next session.

The procedure on Register is invoked whenever the user registers

```
Proc: onRegister
Input: userid
H←GenerateHash(userid);
Tk← getLastUsedToken(userid);
Et←E(H(Tk))
```

B. Securing Register Context

Register context is the important information in the UNI-MOB platform. User hash functions, keys, token and the next expected tokens are all stored in the registration context. To secure this information, hardware solutions like tamper proof storage is available, but it is costly and the user base increases, the solution is not scalable.

To provide security at a low cost and scalable way we propose a solution based on anonymity. The user id is hashed to a location in memory and the hashing operation is conducted in tamper proof storage and in hashed location the registration context is kept. By watching the registration context, no information about user is revealed and it is anonymous. For breaking the anonymity the hashing operation kept at tamper proof storage must be hacked, but it cannot be done as it is secure. Since the registration context is anonymous, the attacker will find it difficult to hack the registration context for a particular user.

C. Continuous Authentication

Due to unlimited packages in call and internet, the session last for even hours in India. In such situations, authentication only during session startup, handover alone is not sufficient, continuous authentication during session is needed.

To ensure continuous authentication, at registration context timer must be kept for a configurable time period and every time period once a attach request is expected from the user end with encrypted token and it is authenticated the same way for handover.

But the hash function has to be updated for better security for the case of continuous authentication instead of using same hash function. But the new hash function must be derived from old hash function by a deviation value sent in attach register.

Piggy bagging can also be done for continuous authentication. The secure hashed token for authentication can be sent attached in data packet so that extra packet need for continuous authentication can be avoid and this will increase the throughput of the system.

In Figure 1 shows the block diagram for third party intervened handover in heterogeneous networks with security. The security block resides inside the UNIMOB system. In over previous work we have presented how UNIMOB takes responsibility of handover by bypassing the authentication from wireless network components. This is the reason, the security is not assured completely. To overcome this drawback, we have introduced security block into UNIMOB.

UNIMOB security block assures three types of security such as replay attack, securing resister context, continuous authentication. The data whenever are tried to exchange between dynamic base stations, the security block will check for their authentication using the three schemes explained above.

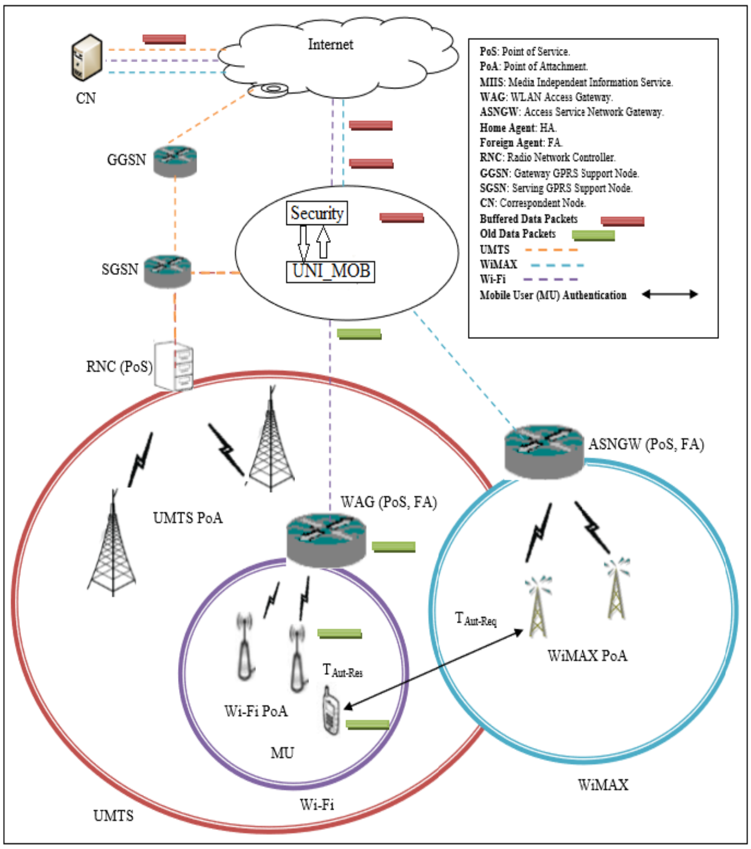

Fig.1. Block Diagram of Proposed Work

IV. MATHEMATICAL MODEL

We model the handover delay due to security additions and is given below

The delay between network component and the UNI-MOB for a packet exchange be : D_{nu}

The delay between UE and the network component for a packet exchange be : D_{en}

The time taken for computing the authentication token at UE be : T_a

The time taken for authenticating the token at the UNI-MOB be : T_{ax}

The network selection delay be : D_n

The time to hash the user to registration context and retrieve the next expected encrypted token be : T_{etx}

The time to calculate the encrypted token at user end is : T_{uex}

The handover delay for UE is modeled as

$$H_u = 2 \times D_{un} + 2 \times D_{en} + D_n + T_a + T_{ax} + T_{etx} + T_{uex} \qquad (1)$$

T_a is dependent on the processing capability of the mobile equipment.

T_{ax} is dependent on the processing capability of the UNI-MOB server and the number of messages queued for processing at UNI-MOB.

$$T_{ax} = T_{fixed} + \sum_{k=0}^{Q} \mathrm{T_{fixed}} \qquad (2)$$

Q is the maximum number of messages that can wait before a message.

Network selection delay is dependent on the number of networks available (N) and the number of attributes (A).

$D_n \propto NA$

V. Result Analysis

Seamless handover across Wi-Fi, WLAN and UMTS is simulated using Java NetBeans IDE 7.2. We measured the handover delay due to proposed authentication mechanism. We compared our solution with our previous work and Gamal work [9].

We varied the number of hosts in steps of 10 for a constant speed of 10 m/s and measured the handover delay as shown in Fig. 2. From the results we find the proposed solution is adding only little overhead to the paper [1] for security, but it is very less compared to Gamal's work [9].

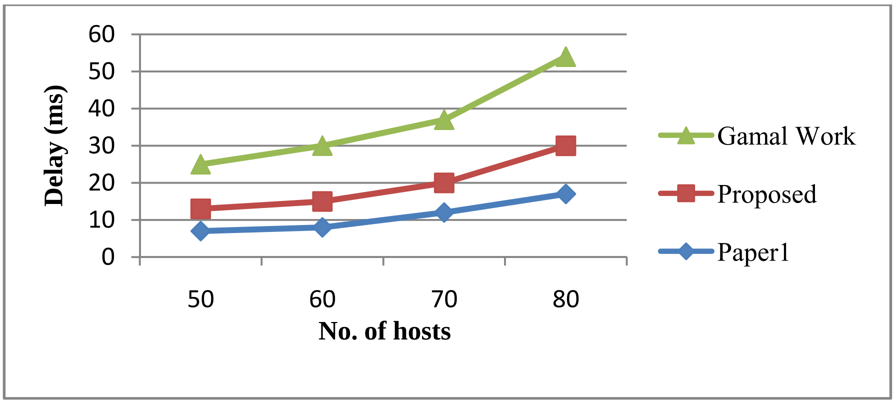

Fig. 2. No. of hosts Vs. Delay (msec)

We varied the number of hosts and measured the network overhead messages in terms of number of messages exchanged between network elements for secure handover and the result is shown in Figure 3. From the result we see that the message overhead in secure handover and paper [1] is almost same but very less compared to Gamal's work [9].

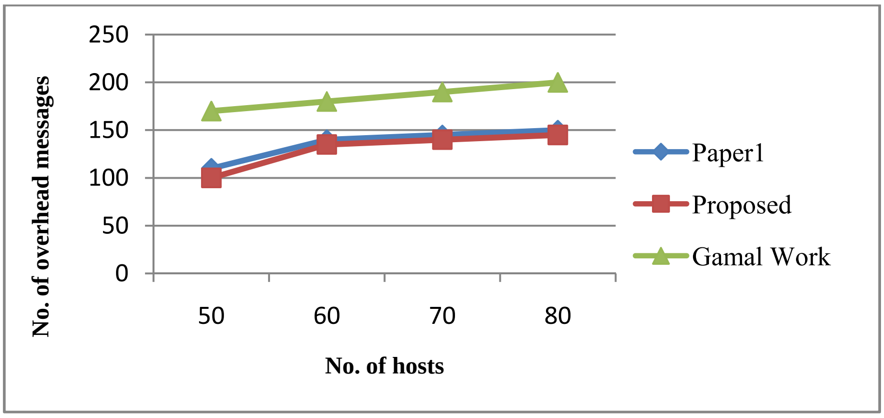

Fig. 3: No. of hosts Vs. No. of message overhead

We varied the speed of a Mobile Station (MS) in a step of 1 m/s and measured the handover delay, the result is shown in Fig.4, From the result we see that delay in proposed is only slightly higher than paper[1] but comparatively very less than Gammal's work [9].

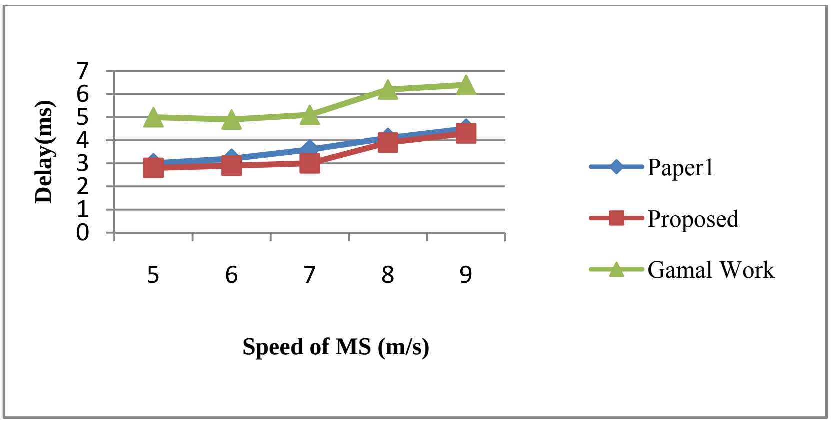

Fig. 4: Speed Vs. Delay

Fig. 5 shows the percentage of packet loss by varying the speed of mobile station, from the result we see that percentage of packet loss is comparatively less than both Paper [1] and Gamal's work[9].

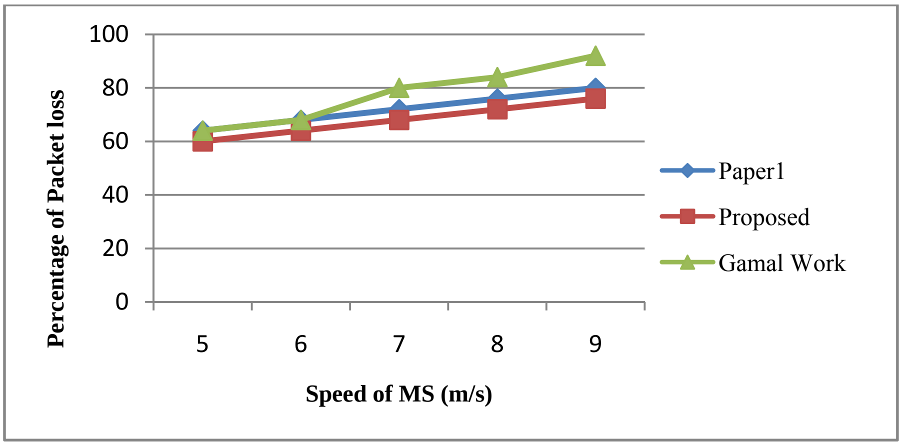

Fig. 5: Speed Vs. Percentage of Packet loss

Percentage of Handover failure rate is measured by varying the speed of mobile station, and the result is shown in Fig. 6. From the result, we see that the handover failure rate is comparatively less than both paper [1] and Gamal's work [9].

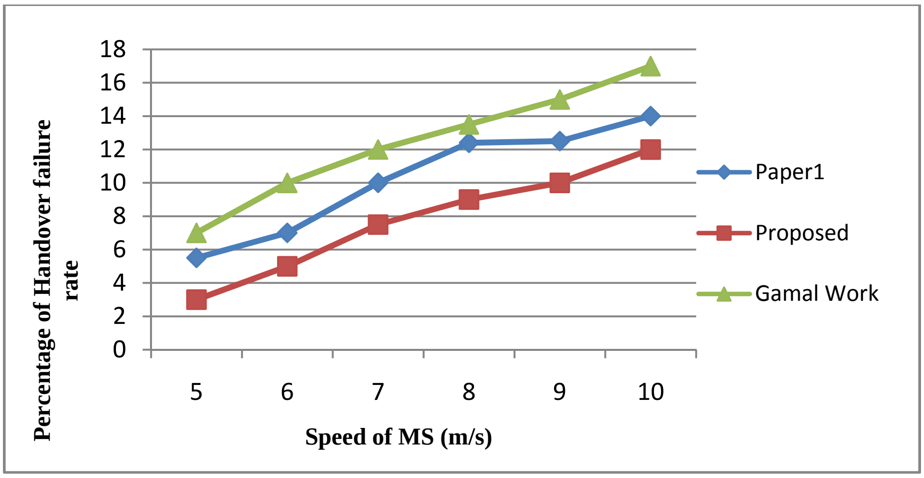

Fig. 6: Speed Vs. Percentage of Handover failure rate

Throughput of the system is measured by varying the speed of mobile station, the result is shown in Fig. 7, From the result we see that the percentage of throughput is higher than paper [1] and Gamal's work [9].

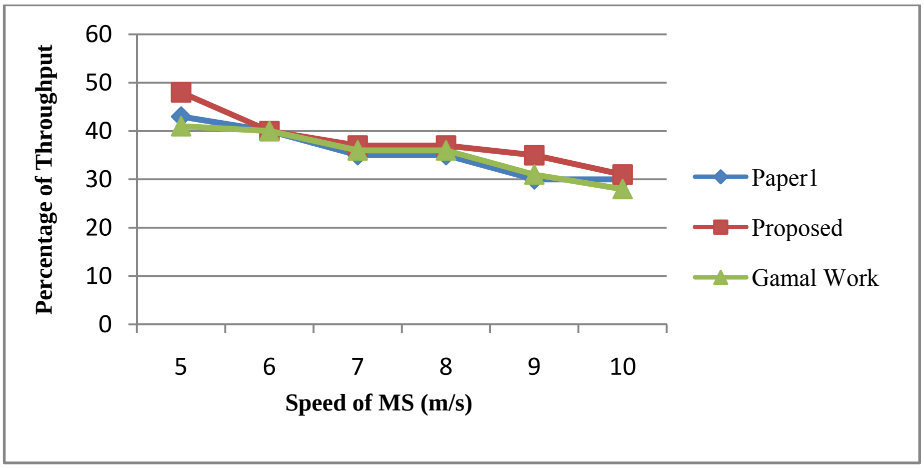

Figure 7: Speed Vs Percentage of Throughput

We measured the effect of replay attack against the number of handover. The effect of replay attack is measured in terms of session drops due to replay attack and the result is shown in Fig. 8. From the result it can seen that proposed security solution has less affect compared to paper [1] and Gamal's work [9].

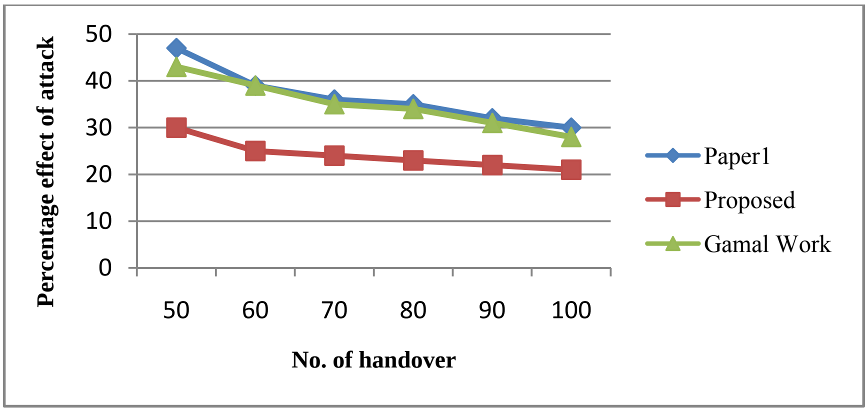

Fig. 8: No. of handover Vs. Percentage affect of attack

We measured the capacity in terms of number of sessions handled by varying the intensity of the attack and the result is shown in Fig. 9. From the result, the number of session handled is high compared to paper [1] and Gamal's work [9].

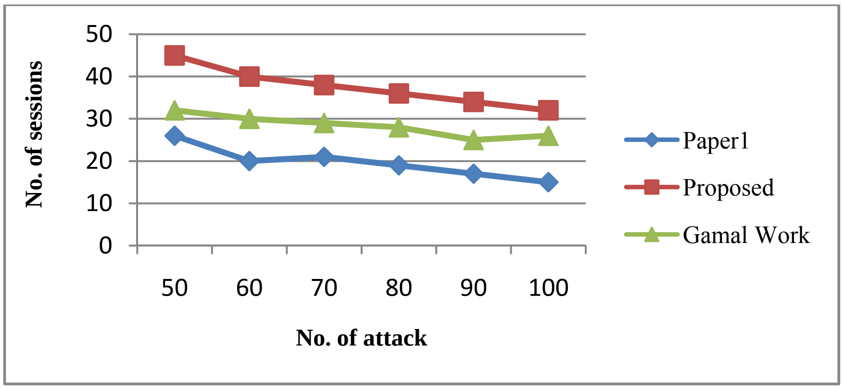

Fig. 9: No. of attack Vs. No. of sessions

We measured the data leakage percentage by varying the number of registration and the result is shown in Fig. 10. From the result, we see that the leakage is less in proposed work compared to both paper [1] and Gamal's work [9].

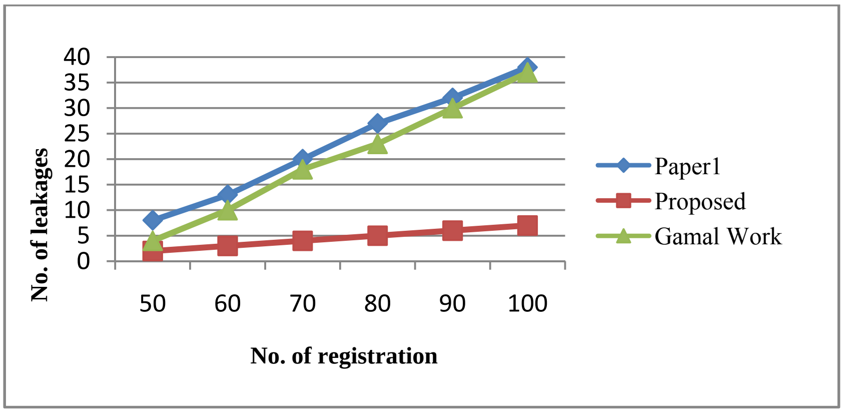

Figure10: No. of registrations Vs. No. of leakages

VI. CONCLUSIONS AND ENHANCEMENT

In this paper, we have given security provision for our previous work, which was third party intervention. After upgrading the third party intervention with security these will overhead and delay issues. Our work has successfully reduced the delay and overhead. Also we have shown at different speeds there is increase in the throughput and decrease in packet loss and handover failure. Overall we have proposed secured third party intervention for present heterogeneous networks.

REFERENCES

[1] S. B. Kumbalavati, J. D. Mallapur, "Third Party Intervened Vertical Handover In Heterogeneous Networks", International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), Vol. 6, Issue 4, pp.1-12, August 2016, ISSN (P): 2250-1568; ISSN (E): 2278-9448.

[2] Ashutosh Dutta, David Famolari, Subir Das, "Media-Independent Preauthentication Supporting Secure Interdomain Handover Optimization", Wireless Communications, IEEE, vol. 15, pp. 55-64, 2008.

[3] Guangsong Li, Qi Jiang,Xi Chen, Jianfeng Ma, "Secure Access Authentication for Media Independent Information Service", EURASIP Journal on Wireless Communications and Networking, 2010.

[4] D. B. Brahim Gaabab, Jean-Marie Bonnint, "Authentication Optimization for Seamless Handovers", IEEE, France, 1-4244-0799-0/07 IEEE 2007.

[5] F. Pereniguez, G. Kambourakis b, R. Marin-Lopez a, S. Gritzalis b, A.F. Gomez, "Privacy-Enhanced Fast Reauthentication For Eap-Based Next Generation Network", Computer Communications, vol. 33, pp. 1682-1694, 2010.

[6] T. Clancy, "Secure Handover In Enterprise WLANs: Capwap, Hokey, and IEEE 802.11 R", Wireless Communications, IEEE, vol. 15, pp. 80- 85, 2008.

[7] Neila Krichene, Noureddine Boudriga, "Securing Roaming and Vertical Handover in Fourth Generation Networks", Proceedings of Third International Conference on Network and System Security, pp.225-231, October 19-21, 2009

[8] Pyung-Soo Kim "New Authentication Mechanism for Vertical Handovers between IEEE 802.16e and 3G Wireless Networks", International Journal of Computer Science and Network Security, Vol.6 No.9B, September 2006

[9] Gamal Abdel Fadeel Mohamed Khalaf & Hesham Zarief Badr "A Comprehensive Approach to Vertical Handoff In Heterogeneous Wireless Networks" Elsevier Journal of King Saud University –Computer and Information Sciences, pp 1319-1578, 2012.

[10] Mahdi Aiash "A Formally Verified AKA Protocol For Vertical Handover In Heterogeneous Environments using Casper/FDR", EURASIP Journal on Wireless Communications and Networking 2012.

[11] Hung-Min Sun, Shuai-Min Chen, Yao-Hsin Chen, Heng-Jeng Chung, I-Hung Lin, "Secure and Efficient Handover Schemes for Heterogeneous Networks", Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference, pp.205-210, December 09-12, 2008.

[12] Wafaa Bou Diab and Samir TohmeSeamless "Handover and Security Solution for Real-Time Services", 11th IEEE International Symposium on Multimedia, 978-0-7695-3890-7/09 $26.00 © 2009

[13] Ahmed H. Zahran and Cormac J. Sreenan "Extended Handover Keying and Modified IEEE 802.21 Resource Query Approach for Improving Vertical Handoff Performance", IEEE 978-1-4244-8704-2/11/$26.00 ©2011

[14] Y. Kim and S. Bahk, "Enhancing Security Using The Discarded Security Information in Mobile WiMAX networks", in Proc. 2008 IEEE Global Telecommunications Conference, pp. 1–5,2008.

AUTHOR PROFILE

Santosh B. Kumbalavati: (b. July 23, 1986) completed his bachelor degree in Electronics and Communication Engineering in 2008 and completed master degree in Digital Communications in 2010 from Vishveshwarayya Technological University (VTU) Belagavi, India. He is pursuing Ph.D. in Electronics and Communication Engineering (2012) from Jain University, Bangalore. His areas of interest are Wireless Communication, Mobile Networks, and Computer Communication Networks etc.

Dr. Jayashree D. Mallapur: (b. Sept. 12, 1969) received Ph.D. in Electronics and Communication Engineering (2009) from Visvesvaraya Technological University Belagavi, India. She is full time professor in the institute of Basaveshwar Engineering College Bagalkot, affiliated to VTU Belagavi. Her current research interests include Wireless Network, Fuzzy Applications, cloud computing and Wireless Sensor Networks. She has published more than 60 National/International papers in conferences /journals. She also has been the chair person of several conferences.