Proceedings of the Pakistan Academy of Sciences:
A. Physical and Computational Sciences: 57 (1): 37-44 (2020)

ISSN: 2518-4245 (print), 2518-4253 (online)

Pakistan Academy of Sciences

Research Article

Optimized Security Context Switching with Low Latency in Vertical Handover

Shah Khalid*, Aftab Alam, and Muhammad Ilyas

Department of Computer Science and Information Technology, University of Malakand, Dir (L), Pakistan

Abstract: Handoff provides seamless mobility to users. When a user crosses the cell boundary of one base station (BS) and enters into the control area of another base station while a call is in progress, this process is called handoff. Horizontal Handoff (HHO) occur if the two base stations use the same network technology while vertical handover occur if the Serving Network (SN) and the Target Network (TN) uses different network technologies. One of the major technical challenges of vertical handover (VHO) is the transferring of security context. In heterogeneous networks the security mechanism of one network is different from other network. Therefore, when a mobile terminal (MT) executes vertical handover, security context with serving network is usually terminated and a new context with target network is created for the mobile terminal. If we securely transfer the old security context in VHO and reuse it with necessary adaptations, then overall latency in VHO will be reduced. In this way a full security context creation is avoided in VHO process and latency is reduced because home network is not involved in the handover process to transfer the security context. This paper presents an algorithm that provide optimized security context switching with low latency in vertical handover process.

Keywords: Handoff, Target Network, Serving Network, Horizontal Handover, Security Context

1. INTRODUCTION

A Cellular system basically consists of three components, the Base Station (BS), Mobile Station (MS) and Mobile Switching Center (MSC). The area under the control of a single BS is called a cell. During a call, when an MS cross the boundary of one cell and enters into the control area of another cell, this process is called handoff. In cellular telecommunications, the term handoff refers to "the process of transferring an active call from one channel to another channel in the target cell. This transformation from current communication channel to new channel could be in terms of time slot, frequency band, or code word" [1].

Handoff decision is mainly based on the relative signal strengths (RSS) from the current BS and neighboring BSs. When the MS moves away from BS, the RSS gets weaker and when the MS moves towards BS, the RSS gets stronger [2]. The handoff process is initiated if RSS from the current BS is lower than the pre-defined threshold and RSS from the neighboring BS is stronger than the pre-defined threshold. The handoff is performed from the current BS to the neighbor BS in order to keep the call active and also to avoid abnormal call termination because of weak signal from the current BS. To improve the overall performance of cellular system, the number of handoffs should be reduced [3], because excessive handovers put heavy handoff processing loads both on Base Stations (BSs) and Mobile Switching Center (MSC). Also, the handoff process requires network resources which increase the probability of dropped calls. Reducing the number of handoffs minimize the switching load and improves the overall performance of the network. Handoff should be avoided if the current BS can provide the desired services.

In order to obtain better handoff service and to reduce the latency the old security context will be

Received: March 2018; Accepted: March 2020
* Corresponding Author: Shah Khalid < khaliddir@gmail.com>

transferred by a little bit adaptation from SN to TN. In this study an overview about the issues related to handoff decision based on security context switching is presented which introduce the concept of middleware that reduces the latency in VHO process.

In section 2, related work has been discussed. In Section 3 the security context is defined. In Section 4 the problems in context switching and their proposed solution are given. Conclusion and future work are given in section 5 and 6 respectively.

2. RELATED WORK

2.1. Types of Handoff

The Handoff can be broadly divided into the following types [4]:

- Hard handoff and Soft handoff
- Intra-MSC handoff and Inter-MSC Handoff
- Horizontal handoff and Vertical handoff

2.1.1 Hard hand off and soft hand off

In hard handoff the MS first releases the channel of the source cell BS and then get a channel from the target cell BS. Thus before making the connection with the target BS, the old connection with the source BS is broken down. For this reason, hard handoff is also known as break-before-make. Hard handoff is implemented in time division multiple access (TDMA) and frequency division multiple access (FDMA) systems such as Global System for Mobile Communications (GSM) and General Packet Radio Service (GPRS) respectively [5].

In soft handoff the MS first gets a channel from the target cell BS and then the channel of the source cell BS is released. The connection to the target BS is made which is utilized by the MT before the connection to the source BS is broken. Therefore, soft handoff is also called make-before-break. Code division multiple access (CDMA) systems such as Interim Standard 95(IS-95) and Wideband CDMA (WCDMA) are based on soft handoff [6].

In hard handoff process the "Ping-Pong" effect is common which is reduced in soft handoff [7]. In a short period of time the MS handoff back and forth, number of times between two base stations. This problem is known as the "Ping-Pong" problem. But the disadvantage of soft handoff is that soft handoff uses multiple connections in the network to support just a single call [8]. Thus the total capacity of the network is reduced as it decreases the remaining free channels.

2.1.2 Intra-MSC handoff & Inter-MSC Handoff

In Intra-MSC handoff both the serving cell BS and the target cell BS are under the control of a single MSC. Handoff occurs between cells which belong to the same MSC's service area. Inter-MSC handoff involves cells that belong to two different MSCs. In this case the serving cell, BS is under the control of one MSC while the target cell BS is controlled by other MSC.

2.1.3 Horizontal Handoff & Vertical Handoff

The handoff which occurs between two network access points that are using the same network technology is called Horizontal handoff (HHO). For example, when a mobile station moves in area covered by multiple GSM base stations, then the handoff among these base stations is horizontal handoff. In other words, horizontal handoff is carried out among homogenous wireless networks and is also called Intra-technology handoff. Vertical handoff (VHO) is a handoff between two network access points, which are using different connection technologies [9, 10]. When a mobile station is transferred from GSM network to WLAN, the handoff performed would be vertical handoff. In other words, vertical handoff is carried out among heterogeneous wireless networks and is also called Inter-technology handoff.

The horizontal handoff decision only depends on the received signal strengths from BSs but in vertical handoff decision, many parameters need to be considered such as different data rates offered, converge areas, access costs, security capabilities, and communication services [11].

2.2. Handoff Strategy

To perform handoff successfully, the handoff process must be initiated at an optimum signal level. Therefore, a slightly stronger signal than the

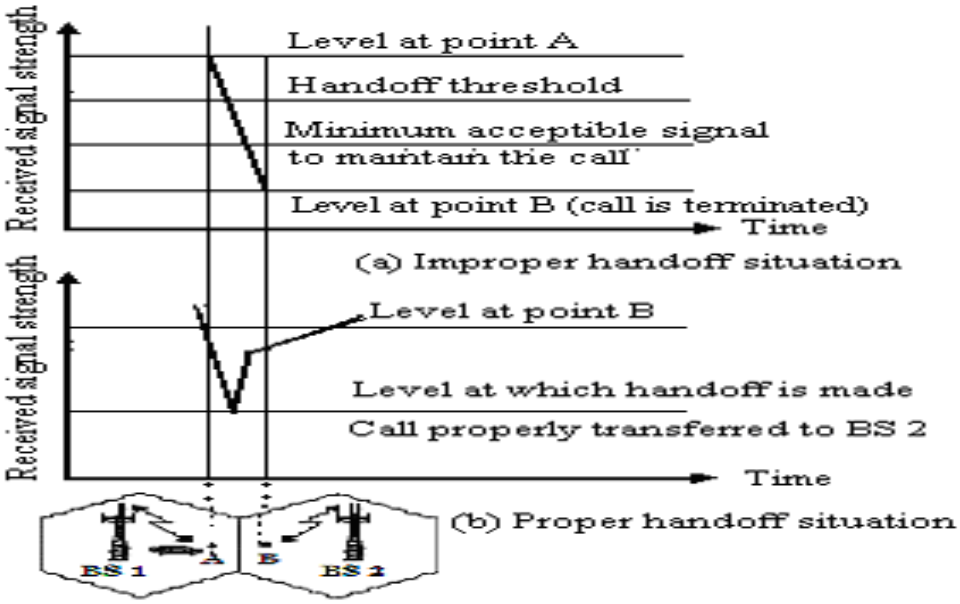

Fig. 1. Handoff strategy [11].

minimum acceptable signal is required for handoff [12]; otherwise the call will be dropped abnormally. This scenario is shown in Fig.1.

In Fig.1 (a), the handoff is not performed at the appropriate signal level; therefore, the call is terminated abnormally. In Fig.1 (b), the handoff is performed at the appropriate signal level. The call is continuing and properly transferred to BS 2.

2.3 Security Context

Security is the top concern in every enterprise's mind today [13]. Basically the security context is used to support trust relationship between SN and TN regarding MT. The main contexts which are used are authentication, authorization, cryptographic transformation techniques for securing the data. In transferring the context, authenticity, security and integrity must be adopted [14-16]. Security context can be created statically as well as dynamically.

In basic contributors of the context switching process in handover are briefly explained [17]:

- **Authentication**

Authentication means to show and prove the identity of peers participating in transaction. In handover process the SN, inform TN and remote SPN about the MT. Then the context will be transfer to TN from SN by the help of remote SPN.

- **Authorization**

The context about the authorization will be transferred from SN to TN about MT. The authorization depends upon on technology and network domain i.e. MT is the partner of SPN are not. Different technology has different level for Quality of service. So, due to different technology and stakeholder, the authorization state need to standardized and formalized to avoid misunderstanding between SN and TN.

- **Cryptography (secrecy of data and user)**

The security context transformation process can be made secure by using some strong cryptographic algorithms [18].

3. PROBLEMS IN CONTEXT SWITCHING AND PROPOSED SOLUTIONS

In security context transferring the following problems are identified during handover process:

i. The MT has a few identifiers for subscription and that will be transferred to TN, so his privacy and the commercial SPN secrecy will be compromised due to low security standard of the TN.
ii. If the MT uses different subscription to access SN and TN services, then it is very difficult for the SN to give or transfer a meaningful indication to TN about MT.

iii. Function of different networks is different for different communication; this will create problem in context switching for example mutual authentication in 3G is not provided by WEP 802.11 b.
iv. The stakeholder trust level is also different.
v. Due to different technology and Different stakeholder the authorization state need to standardized and formalized to avoid misunderstanding between SN and TN (Authorization problem).
vi. In request transfer scheme the denial of service issue is created.

4. PROPOSED SOLUTION

Next generation networks also called 4G networks are the emerging networks which will provide high data transfer rates, quality of services and seamless mobility to their users. The different heterogeneous networks each offering different services to the user will be combined into a single network. Users will be able to switch among different networks based on their preference, which is called VHO. In this connection the SN send request to the SPN to which the SN is connected to transfer the security context to TN. The SPN first of all check the TN registration with himself. If both users i.e. SN and TN registered with the same SPN, then the process of HHO is performed with AAA. If the SN and TN not registered with same SPN, the MSC will contact the middleware. A middleware will be an authentic body on which all the entities in a given domain have a trust on it and it facilitate the communication among the entities for handover process. The middleware will work is a single standard for different heterogeneous networks and it will integrate them into a single platform. The middleware can also play his role in security context transfer by using some strong stream or block ciphers and further providing natural language security for encryption and decryption [19].

The mentioned problems can be resolved with the help of a middleware. The middleware firstly checked the security context of SN and TN and

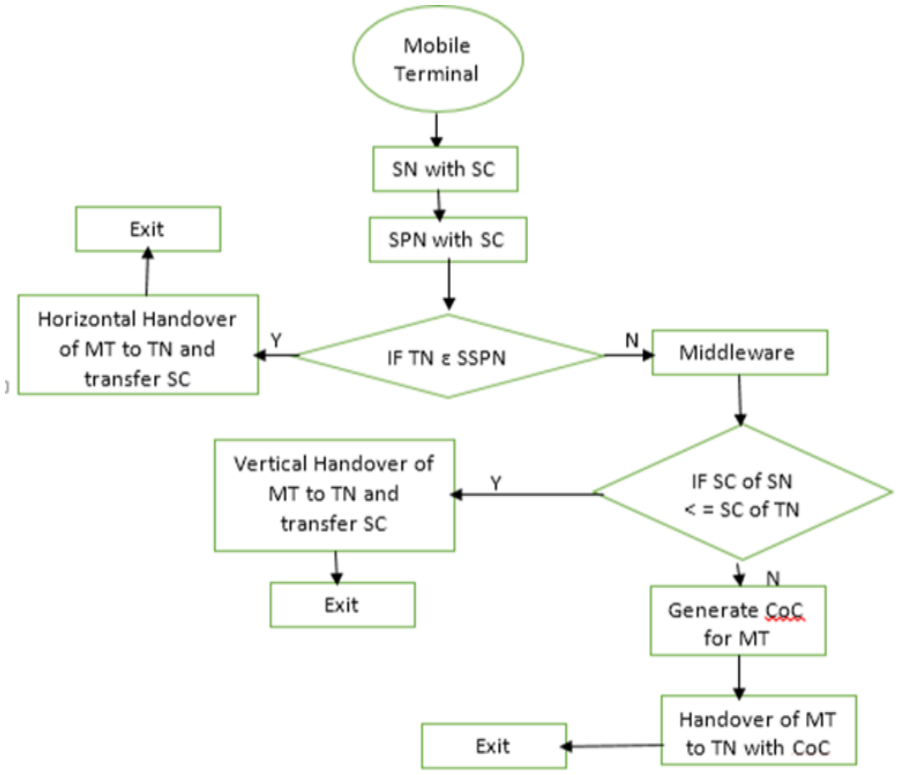

Fig. 2. Flow Chart of the proposed Algorithm

compare them. If the SN context is less than the TN then vertical handover is occur if not then Middleware generate care of context for SN. The algorithm for transfer of security context in VHO process is explain in the following lines along with flow chart as shown in Fig.2.

Algorithm: Security Context Switching (Security Context (SC), Serving Network (SN), Target Network (TN), Mobile Terminal (MT), Service Providing Network (SPN), Same Service Providing Network (SSPN), Authorization, Authentication and Accountability (AAA).

This algorithm is used to transfer the security context in handover process. SC is the Security Context, SN is the Serving Network, TN is the Target Network, SPN is the Service Providing Network and SSPN is the Same SPN. AAA is Authorization, Authentication and Accountability server which involve in handover:

- SN send a request to SPN of Handover to TN.
- SPN check for TN registration with itself
- If (SN and TN ε SSPN Then:
  Handover is performed with AAA of SN to TN and Exit // Horizontal Handover
  Else: SPN contact Middleware (MDW_{ASI})
  [End of if structure]
- MDW_{ASI} checks and compare the security context of SN and TN when SN ε SPN1 and TN ε SPN2
- if (SC of SN <= SC of TN) Then:
  Handover is performed with AAA of SN to TN and Exit.

  Else:

MDW ASI Generate Care of Context (CoC) for MT and send it to TN for communication.

[End of if structure] //CoC means Care of Context

- VHO is performed with CoC. MT and TN communicates with each other through MDW_{ASI}
- Exit

Main requirements for context transfer are authentication, authorization, transfer of information in a secure way and built the trust between the entities involved in handover process. To achieve the above mentioned security the proposed algorithm transfers the context between the entities involved in handover process after being analyzing the security standard of the involved entities. The algorithm makes the context standardized with the help of a middleware according to the best one standard used by one of the two entities. The middleware generates the CoC which optimize the existing context of the TN for SN. The middleware CoC generation process takes less time (it add some additional context to the original) as compare to regeneration of context from the scratch. It reduces the overall latency. The authentication, authorization and trust establishment process will be performed in SPN and middleware.

5. CONCLUSION

Next generation networks also called 4G networks are the emerging networks which will provide high data transfer rates, quality of services and seamless mobility to their users. The different heterogeneous networks each offering different services to the user will be combined into a single network. Users will be able to switch among different networks based on their preference. The process of switching among different networks is called Vertical Handover. The vertical handover face different challenges which must be handled properly in order to successfully execute the handover process.

5.1 Security

In vertical handover the most important issue is security. A user that requires high security will not prefer a network which has low security even if the target network has better services than the serving network. In this paper the concept of Middleware is presented which transferring the security context during vertical handover process. If the security of the target network is less than the security of the serving network the middleware generate high security context for the MS dynamically and execute the handover process securely that full fill all the security requirements of the MS in the new domain.

5.2 Handover Latency

During vertical handover much times is consumed in identifying the services of the target network. Also multiple messages must be exchanged between the source network and the target network before the handoff is performed. This increases the latency in the handover process which is not desirable and effect the efficiency of the network. The middleware is aware of the services of different networks and there is no need of large communication between the serving network and the targeted network for the handover process. Most of important tasks are performed by the middleware on behalf of serving network and target networks. So the overall communication is reduced which ultimately reduces the overall latency in the vertical handover process.

6. FUTURE WORK

Vertical handoff will remain the challenging issue in the 4G networks due to the mobility of users utilizing the services of different heterogeneous networks. In the integration of heterogeneous wireless networks, there are many problems that need to be further investigated. Some of these problems are load balancing and traffic management among networks, Quality of Service support during vertical handoff, resource sharing and resource allocation, security and authentication, billing and operator agreements and implementation details.

In this study we presented the concept of middleware for securely transferring the security context and reducing latency in vertical handover process. The future work must address the overall structure of the middleware, its different components and how they will communicate with different networks. It should also determine the type of protocols that will be used by the middleware to integrate heterogeneous networks into a single logical network.

7. REFERENCES

1. N. Ekiz., T. Salih, S. Kucukoner and K. Fidanboylu. An overview of handoff techniques in cellular networks. *International journal of information technology* 2(3): 132-136 (2005).
2. X. Ma., Y. Cao, Y. Liu and K.S. Tarvidi, Modeling and performance analysis for soft handoff schemes in CDMA cellular systems. *IEEE Transactions on Vehicular Technology* 55(2): 670-680 (2006).
3. N. Nasser., A. Hasswa, and H. Hassanein. Handoffs in fourth generation heterogeneous networks. *IEEE Communications Magazine* 44(10): 96-103, (2006).
4. V.K. Garg, and T.S. Rappaport, Wireless network evolution: 2G to 3G, Prentice Hall PTR, (2001).
5. A.E. Leu, and B.L. Mark. Modeling and analysis of fast handoff algorithms for microcellular networks. Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002. *Proceedings. 10th IEEE International Symposium on, IEEE* (2002)
6. N.D. Tripathi., J.H. Reed, and H.F. VanLandinoham. Handoff in cellular systems. *IEEE personal communications* 5(6): 26-37 (1998).
7. D. Wong, and T.J. Lim. Soft handoffs in CDMA mobile systems. *IEEE Personal Communications* 4(6): 6-17(1997).
8. X. Ma., Y. Liu and K.S. Trivedi. Design and performance analysis of a new soft handoff scheme for CDMA cellular systems. *IEEE Transactions on Vehicular Technology* 55(5): 1603-1612 (2006).
9. L.J. Chen., T. Sun, B. Chen, V. Rajendran, and M. Gerla, A smart decision model for vertical handoff. Proceedings of the 4th International Workshop on Wireless Internet and Re-configurability, Athens, Greece, (2004).
10. A. Mahmood., S. M. Hilles, and H. Zen. Vertical Handover Decision Schemes in Fourth Generation Heterogeneous Cellular Networks: A Comprehensive Study. *International Journal of Business Data Communications and Networking (IJBDCN),* 14(1) 1-26 (2018).
11. E. Stevens-Navarro., U. Pineda-Rico, and J. Acosta-Elis. Vertical handover in beyond third generation (B3G) wireless networks. *International Journal of Future Generation Communication and Networking* 1(1): 51-58 (2008).
12. T.S. Rappaport. Wireless communications: principles and practice, prentice hall PTR New Jersey (1996).
13. G.M.D.T. Forecast. Cisco visual networking index: global mobile data traffic forecast update, 2017–2022. Update, 2017: 2022 (2019)
14. P. Nikander, and L. Metso. Policy and trust in open multi-operator networks. Telecommunication Network Intelligence, *Springer:* 419-436, (2000).
15. I. Bisio., A. Sciarrone. Fast multiattribute network selection technique for vertical handover in heterogeneous emergency communication systems.

Wireless Communications and Mobile Computing (2019).

16. S. Kalpana., S. Chandramathi. Authentication based on blind signature and ring signature algorithms during vertical handover in heterogeneous wireless networks. *Cluster Computing.* 22(5) 12037-12047 (2019).
17. H. Wang, and A.R. Prasad. Security context transfer in vertical handover. Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th *IEEE Proceedings on IEEE* (2003).
18. W. Stallings. Cryptography and Network Security 2nd edition, p 23-24, Prentice-Hall, Inc. ISBN 0-13-869017-0 (1999).
19. M. Salam., N. Rashid., S. Khalid, and M.R. Khan. A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case). *World Academy of Science, Engineering and Technology.* 73 (2011).