SIDP: A Secure Inter-Domain Distributed PMIPv6

Muhammad Zubair, Xiangwei Kong, Saeed Mahfooz, and Irum Jamshed

***Abstract*—Proxy Mobile IPv6 (PMIPv6) offers centralized network-based mobility support for mobile nodes (MN). This centralized nature of mobility leads to the performance issues such as single-point failure, non-optimal routing, low scalability, authentication latency, and signaling overhead. Additionally, PMIPv6 does not support inter-domain handover due to which the on-going sessions cannot be maintained between two PMIPv6 domains. The existing solutions for inter-domain mobility management are considered to be unsuccessful to cope with this problem. In this paper, a novel approach called Secure Inter-domain Distributed PMIPv6 (SIDP) is proposed to overcome the aforementioned issues. The SIDP separates traditional mobility anchors into Control Mobility Anchor (CMA) and Data Mobility Anchor (DMA). CMA holds the functionalities of Mobile Access Gateway (MAG) and control plane whereas DMA buffers and forwards the data plane packets. We present basic design, DMA decision process, strong authentication, dynamic mobility management, optimized routing, and inter-domain handover of our proposed scheme. The authentication procedure is based on symmetric cryptographic and collision free one-way hash function to make the distributed mobility management secure. The security analysis demonstrates that the proposed scheme possesses user anonymity, fraud avoidance, mutual authentication, forward secrecy, backward secrecy, and one-time session key agreement.**

***Index Terms*—Authentication, centralized mobility management, distributed mobility management, inter-domain handover, Proxy Mobile IPv6.**

I. Introduction

Substantial advancement in hardware and wireless technologies has made the proliferation of mobile devices affordable to massive user community over the past few years [1]. Besides this, the mobile data traffic has histrionically increased due to a vast number of users enjoying an assortment of applications in mobile devices such as video streaming, instant messaging, online gaming, social networks, and web surfing. The research communities are putting their efforts to make the future networks capable of withstanding the users' demands and technologies evolution [2].

Currently mobile networks are sprouting from the third generation (3G) to fourth generation (4G) to efficiently address the user demands regarding mobile broadband traffic. IP mobility management is considered as an important feature in the designs of future networks. Recently, the Third Generation Partnership Project (3GPP) and WiMAX have widely adopted Proxy MIPv6 PMIPv6) which has been standardized by Internet Engineering Task Force (IETF). PMIPv6 experiences network-based approach to manage the IP mobility for Mobile Nodes (MN) without their immersion. Network-based mobility management comes up with certain advantages as compared to host-based mobility management (e.g. Mobile IPv6, Fast MIPv6, and Hierarchical MIPv6). These are; minimizing tunnel overhead and reducing handover latency, mobility management support without the participation of MN, and evading the complications of protocol stack in the MN. Though, the inter-domain mobility is still a challenge in PMIPv6 which means the session cannot be continued during the MN movement from one PMIPv6 domain to another [3].

Inter-domain mobility has been focused in several approaches such as integration between MIPv6 and PMIPv6 (H-PMIP) [4], and Inter-Domain Mobility Extension for Proxy-Mobile IP (I-PMIP) [5]. However, severe issues like signaling overhead, handover latency, sub-optimal routing, lack of dynamic mobility management, and authentication latency make these inefficient. Particularly, the centralized nature of mobility management in PMIPv6 leads to single point failure and the above mentioned limitations. In [3] a distributed approach has been adopted to support inter-domain in PMIPv6, but the inclusion of Inter-domain Central Mobility Database (ICMD) incurs handover latency and signaling overhead due to extra binding operations with ICMD before the tunnel establishment between previous Local Mobility Anchor (LMA) and the current LMA. Further, relying on central entity makes it an easy to be attacked by an intruder. They have also considered the fully distributed approach in which the ICMD has been removed, but it has been declared complex and having higher signaling cost by the authors of this approach.

The limitations due to centralized nature of mobility management motivate Distributed Mobility Management (DMM) which is currently a quite hot topic in both research and standard communities. DMM is evolving the existing mobility system to flatter architecture, which deploys the mobility anchors closer to the users. Judgmentally, we can say DMM is making MN capable of something which is not possible through existing centralized schemes. Moreover, it is expected to be easily deploy the DMM by removing all the complexities in centralized mobility management [6].

In this paper, we propose a novel approach called Secure Inter-domain Distributed PMIPv6 (SIDP). The control and data plane are separated in our proposed scheme in order to attain the purposes of distributed mobility management effectively. Dynamic mobility and optimal route are maintained during handover process of MN from one PMIPv6 domain to another. Additionally, for the secure

Manuscript received October 26, 2013; revised December 19, 2013.

Muhammad Zubair and Xiangwei Kong are with the School of Communication and Information Engineering, Dalian University of Technology, China (e-mail: m.zubairpaf@gmail.com, kongxw@dlut.edu.cn).

Saeed Mahfooz is with the Department of Computer Science, University of Peshawar, Pakistan (e-mail: saeedmahfooz@upesh.edu.pk).

Irum Jamshed is with the Institute of Management Sciences, Peshawar Pakistan (e-mail: irum.jamshed@gmail.com).

handover procedure we introduce an efficient authentication mechanism in our proposed scheme, based on symmetric cryptographic and collision free one-way hash function. The main contributions of this paper are designing of secure inter-domain approach which have; lower handover latency between PMIPv6 domains, optimized routing, enhance scalability, avoidance of single point failure, minimize signaling overhead, prevention of packet loss, and an efficient authentication.

The rest of this paper is structured as follows; Section II covers a summary of previous and current research on inter-domain mobility management and concept of DMM. In Section III, the proposed scheme is described, followed by security analysis in Section IV. Finally, conclusion and future work are presented in Section V.

II. Related Work

The basics of designing any internetwork are to understand the existing mobility solutions, the motivation behind their design, and their performance regarding the existing architecture of internet. In this section we consider the existing mobility solutions for inter-domain mobility in current internet architecture, followed by distributed mobility management approach in both research and standard communities.

The mobility protocols of both host-based and network-based can be categorized into intra-domain or inter-domain protocols (e.g. micro mobility or macro mobility) based on the scope [7]. Operationally these protocols views networks and mobile devices in a different way depending on the fundamental principles of mobility management. Among the major mobility protocols (such as MIPv6, FMIPv6, and HMIPv6), the PMIPv6 is considered an efficient solution for future networks. But, the support of inter-domain mobility is still an issue in PMIPv6 for the session continuity between domains. Several approaches have been proposed having a common idea of using global mobility anchor to handle the MN movement to visited PMIPv6 domain. A hybrid solution of MIPv6 and PMIPv6 is proposed in [4], which has used PIMIPv6 as an intra-domain mobility management and MIPv6 as a global mobility management. The increase in complexity of the hosts makes this approach inefficient due to the support of protocol stacks for both host-based and network-based mobility management. Additionally, the co-location of MIPv6 and PMIPv6 at HA/LMA is also considered. However, the natural variations between both protocols result several problems [4].

An extension for the support of inter-domain mobility in PMIPv6 (I-PMIP) is proposed in [5], which has reused the local mobility anchor as a global mobility anchor during MN movement to visited domain. Two types of mobility anchors such as Session Mobility Anchor (SMA) and Serving Local Mobility Anchor (S-LMA) are used to manage the traffic. The critical issue with this approach is the per user basis providence of mobility service. Hence, the sessions which do not require mobility support also get the mobility service. Additionally, MN has to use the SMA as an anchor when it initiates new session at a new domain, this may result issues such as sub-optimal routing and tunnel overhead. In [8] the proposed solution has used both home address (HoA) and Care-of-Address (CoA) not only for MN, but also for particular session. Each entity that belongs to PMIPv6 upholds two types of Binding Cache Entry (BCE) such as Inner-Domain BCE and Inter- Domain BCE for every MN which has registered. During MN handover from one PMIPv6 domain to another, the serving LMA has to communicate with the previous LMA and home LMA to obtain the HoA of CN and can update the current location of MN respectively. In case of CN, when it changes the PMIPv6 domain, the same process is performed. Although efforts are putted to route the traffic in optimal way, but it becomes too complex when the communication has to perform at the same time with many CNs. Further, this solution is only feasible where the MN and CN belong to PMIPv6 domains.

The centralized approaches which consider both intra-domain and inter-domain mobility lead to several issues such as single-point failure, non-optimal routing, low scalability, authentication latency, and signaling messages overhead of the mobility protocols [9]. In order to overcome these issues, recently IETF has introduced a new solution that is Distributed Mobility Management and opened a working group in this regard. The aims and objectives of this group is to distribute the mobile internet traffic in optimized manner and not to be depend on centralized approaches [6], [10]. Although, the DMM concept is in early phase of standardization, still we present some proposed approaches which are known to our knowledge. In [11], [12], the proposed solutions have focused on distributing the traffic volumes of data plane. The MNs inside same domain can communicate directly by defining new messages for binding query and response. But in the case of outside the domain, there is still a single LMA having control and data plane to communicate MN and Correspondent Node (CN). A Net-based DMM is presented in [13] which have a central mobility database acting as a control plane anchor to process all the signaling messages without considering the concept of domain. In [14] the DMM with MIP and Proxy MIPv6 is proposed, which placed the location management (LM) with HAA or separately. This can results extra signaling latency during frequent handover if mobility routing (MR) and LM are located at much distance. The distributed mobility approach based on PMIPv6 presented in [15] has used MAG to communicate with Control plane Local Mobility Anchor (CLMA) and Data plane Local Mobility Anchor (DLMA). Because of this, extra latency and signaling overhead can be resulted if the MAG, CLMA, and DLMA are located far away during the frequent handover. Additionally, the centralized AAA server authenticates the MN, which results the increase in latency.

The distributed approaches up till now only focused on mobility management, none of these have considered the authentication mechanism in distributed manner. Hence, considering distributed mobility management, there is also a need to focus on the authentication mechanism.

III. Proposed Scheme

The proposed scheme called Secure Inter-domain Distributed PMIPv6 (SIDP) manages mobility using the

concept of PMIPv6. Architecture of SIDP is presented in Fig. 1 which improves PMIPv6 by making the mobility distributed. Both the control and data planes of centralized mobility anchor are separated into Control Mobility Anchor (CMA) and Data Mobility Anchor (DMA). The CMA incorporates the functionalities of Mobile Access Gateway (MAG) and control plane. The control plane includes signaling messages of binding registration, maintaining Binding Cache Entry (BCE), allocation of home network prefix (HNP) and DMA to MN. The DMA has the responsibility to buffer and forward the Data Plane packets. There can be multiple CMA and DMA in a single network to accommodate mobile nodes in large number. Furthermore, efforts are also made to distribute the three logical functions of LMA as described in [14]. This distribution of logical functions, control and data planes enables SIDP to achieve the main purposes of distributed mobility management. A strong authentication procedure is incorporated in proposed scheme which is based on symmetric cryptographic and collision free one-way hash function to secure DMM as justified in security analysis in Section IV.

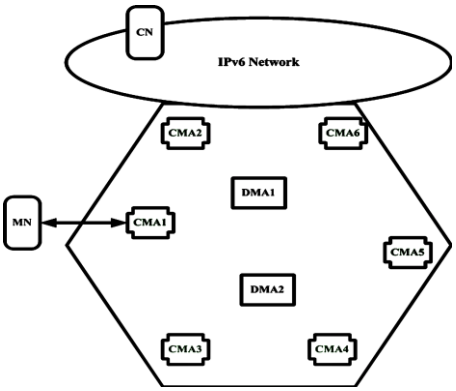

Fig. 1. Architecture of SIDP.

A. Basic Design

The process of accessing CMA by MN and delivering the packets to CN is presented in basic design of SIDP as shown in Fig. 2. In the proposed scheme, the MN is attached to CMA just like the attachment of MN to MAG in PMIPv6. The major difference is that CMA selects DMA for each MN. The whole process is presented in details below.

1) The MN first attaches to CMA by sending router solicitation (RtSol) and login (M_1) message. Authentication of MN and M_1 is explained in subsection C. After the successful authentication, the CMA would obtain the profile of MN having MN's ID and other information.
2) As the functionalities of MAG and control plane are incorporated in same CMA, the PBU and PBA messages are managed locally. The CMA allocates Home Network Prefix (HNP), assigns DMA based on decision procedure of DMA as explained in subsection B, and generates the binding cache entry (BCE) for MN.
3) The CMA sends the HoA-to-PCoA mapping message to DMA for registration. A new flag 'D' is added to the message format which must be zero to indicate that it is the registration message for HoA-to-PCoA mapping [14].
4) A bi-directional tunnel is established between CMA and DMA, and then route is setup over the tunnel for home network prefix of MN.
5) The router advertisement (Rtr Adv) message is sent to MN by CMA which includes HNP through which the MN configures its home address (HoA).
6) The steps 6-8 in Fig. 2 show the flow and format of data plane packets for our proposed scheme which is quite similar to PMIPv6. The main difference is the replacement of LMA address field with DMA address field. The plain arrow represents signaling whereas the dotted arrow represents data plane packets.

Notice that, in order to process the encapsulated packets from CMA, the DMA directly deprives the outer header and then forward it.

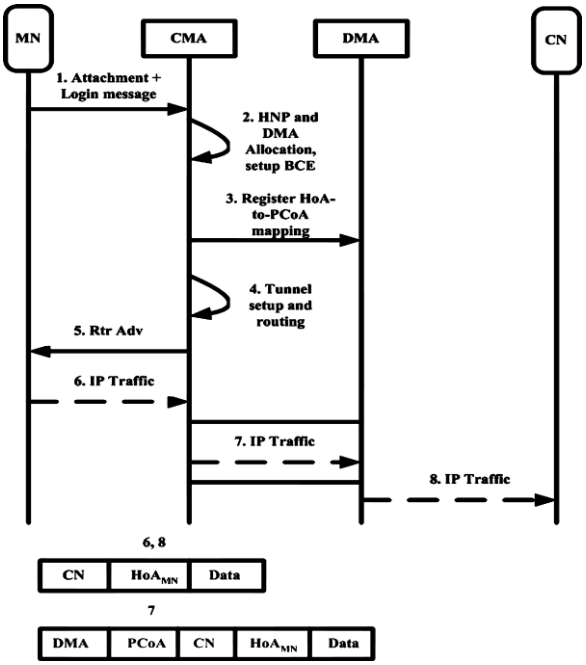

Fig. 2. Basic design for deployment of SIDP.

B. DMA Decision Process

The CMA takes the decision of selecting DMA upon the attachment of MN, which refers to the decision process of DMA in our proposed scheme. The decision is made on number of hops between CMA and DMA, and the load of DMA. The light load DMA nearby to CMA would be selected for MN. It is assumed that CMA knows the distance between itself and each DMA. Let $H_{CMA\text{-}DMA}$ denotes the number of hops between CMA and DMA. The minimum number of hops represents the closest DMA to CMA.

In order to compute the load of DMA, we suppose that BD_{MN} is the bandwidth utilization for each MN, and BD_{DMA} represents DMA total bandwidth. The MAX_{MN} is the value for DMA representing maximum numbers of MN which should not be surpassed. Thus, the MAX_{MN} must be less than BD_{DMA}/BD_{MN}. The DMA is checked for number of assigned MNs', if it is less than MAX_{MN}, the L denotes load is assigned value 1 else 0. The decision of DMA is expressed as

$$DMA_{\text{Dec}} = L \times min\ (H_{\text{CMA-DMA}})$$

The CMA selects the DMA for MN which has L equal to 1 and minimum number of hops between itself and DMA.

C. Authentication

The authentication procedure for SIDP comprises of five phases; registration, login, authentication, session key update, and password change. In Table I, the descriptions of different notations used in the authentication process are presented. The high-entropy random numbers based master secret keys of 256 bits in length such as X_{CMA} and X_{DMA} are assumed to be held by each CMA and DMA. Before the start up process of authentication, long term common secret keys of 126 bits in length are shared among entities using Diffie-Hellman key agreement protocol [16]. Our proposed scheme uses collision free one-way hash function which produces output having 160 bits. The further explanation of authentication procedure is demonstrated in following phases.

TABLE I: NOTATIONS

Symbol	Description	Symbol	Description
ID_{CMA}	Identity of CMA	R_{MN}	Random numbers selected by MN
ID_{MN}	Identity of MN	TK	Temporary key
PWD_{MN}	Password of MN	sk	Session key
F	Fingerprint	X_{DMA}, X_{CMA} K_{MN}	Common secret keys for DMA, CMA, and MN
TS_{MN}	Timestamp generated by MN	r_{MN}	Random number of m-bit
$\oplus$	XOR operator	$PCert_{MN}$	Provisional certificate
$\|\|$	A concatenation operator	$H(\cdot)$	A collision free one-way hash function

Registration Phase: The MN chooses password PWD_{MN} of 8 bytes in length, random number R_{MN}, and fingerprint F. A password PWD_{MN} may comprise of characters or digits. The MN calculates $h(PWD_{MN} \oplus R_{MN} \oplus F)$ and submits its ID_{MN} having 128 bits in length to CMA through secure channel. After receiving ID_{MN} from MN, the CMA performs the following operations.

1) The $SID = (ID_{CMA} \oplus ID_{MN})\ X_{CMA}$ and $K_{MN} = h(ID_{MN} \| X_{CMA} \| r_{MN})$ are calculated, where r_{MN} in K_{MN} represents secret value of length l, which is randomly selected for each MN by CMA. For the encryption, we use RC5 as a symmetric algorithm having plain text of length L bits. Thus, the length of cipher text must be: $\left\lceil \frac{L}{128} \right\rceil \times 128$

   Here, 128 is the bit length of ID_{CMA}.
2) A smart card which comprises of $\{SID_{MN}, K_{MN}, h(.)\}$ is issued by CMA to MN through secure channel.
3) The MN computes the followings after receiving smart card;

$$V_{MN} = K_{MN} \oplus h(ID_{MN} \| h(PWD_{MN} \oplus R_{MN} \oplus F)$$
$$H_{MN} = h(h(K_{MN}))$$

The K_{MN} is replaced with $\{V_{MN}, H_{MN}\}$ by MN, and enters its own R_{MN} and F to the smart card. Finally, the smart card comprises of $\{V_{MN}, H_{MN}, SID_{MN}, h(.), R_{MN}, F\}$.

Notice that the scanning component is assumed to be built-in inside MN in order to obtain digital fingerprint value. If the MN does not have fingerprint scanning component, then the hash value $h(PWD_{MN} \oplus R_{MN})$ will replace $h(PWD_{MN} \oplus R_{MN} \oplus F)$ in our proposed mechanism.

Login Phase: The smart card is inserted into the device by MN and enters its ID_{MN}, password PWD_{MN}, and fingerprint F. Then, the smart card performs following operations.

1) Computation of $K_{MN}=V_{MN} \oplus h(ID_{MN}\|h(PWD_{MN} \oplus R_{MN} \oplus F)$ and $H^*_{MN} = h(h(K_{MN}))$
2) The condition is checked whether H^*_{MN} is equal to H_{MN}. If it becomes equal, the MN is declared legal and proceeds to the next step. In the case if H^*_{MN} is not equal to H_{MN}, the login request is rejected.
3) Computation of $E = (h(ID_{MN}) \| ID_{CMA} \| n_0)TK_{MN}$ where TK_{MN} *is* temporary key and calculated as $h(TS_{MN} \oplus K_{MN})$. The ID_{CMA} denotes the identity of CMA to which MN wants to login. The n_0 represents secrete random number of 256 bits in length which is selected by MN to create session key between MN and CMA. TS_{MN} means time stamp, assumed to be 64 bits in length and it is used by MN to resists against replay attacks.
4) The login message includes $M_1 = \{SID_{MN}, E, TS_{MN}\}$ which is sent to CMA.

Authentication Phase: The following operations are performed by CMA to authenticate the MN.

1) After getting login message M_1 from MN, CMA checks time stamp TS_{MN}. If it is found expired and invalid, then the login request is rejected. Otherwise, CMA obtains ID_{MN} through X_{CMA} by decrypting SID_{MN} and checks its format. In the case of valid format, CMA computes $K_{MN} = h(ID_{MN} \| X_{CMA} \| r_{MN})$ and generates $TK = h(TS_{MN} \oplus K_{MN})$ using ID_{MN}. Subsequently, the message E is decypted by CMA and obtains $\{h(ID^*_{MN}), ID^*_{CMA}, n_o)\}$ through TK_{MN}. The $h(ID_{MN})$ is computed by CMA, and checks whether it is equal to $h(ID^*_{MN})$. If it is equal, it ensures that the MN and its TS_{MN} is legal and CMA generates session key $sk = h(h(K_{MN}) \| n_0)$. If not, the MN is declared illegal, and the authentication is terminated.
2) The message M_2 is sent to MN by CMA which comprises of $\{PCert_{MN} \| h(n_o))_{sk}$ after ensuring the validity of MN in step 1. The $PCert_{MN}$ represents provisional certificate having 256 bits of length containing life time and other information.
3) The MN upon receiving M_2 and router advertisment computes session key sk, obtains $PCert_{MN}$ and n_0 by decrypting M_2. The $h(n_0)$ is compared with $h(n\times_0)$ to check the legality of CMA. If it is found legal, it means the MN is communicating with its own CMA.

Notice that the authentication procedure between CMA-CMA and CMA-DMA will be same comprises of their own IDs', time stamps, and the session keys.

Session Key Update Phase: In order to improve efficiency and ensure strong secuirty, periodic updation of session is performed by the following operations.

The MN is assumed to be in i^{th} session and it sends a message $\{PCert_{MN}, (n_i \| PCertMN \| Additional\ information)_{ski}$ to CMA. The message is encrypted with i^{th} session key $sk_i = h(h(K_{MN} \| n_i\text{-}1)$, where $i = 1, 2, 3, \ldots\ldots, N$. CMA decrypts the message, if MN is found valid, then n_i is

saved as a new session key for upcoming messages.

Password Change Phase: The password PWD_{MN} can be changed with the new password PWD_{MNnew} by performing the following steps.

1) Firstly, the steps 1) and 2) in login phase must be performed.
2) If the legality of MN is insured, then MN enters $\{PWD_{MNnew}, R_{MNnew}, F\}$ and request for new password. In the other case, if MN is not legal, the password change request is rejected.
3) The smart card in MN calculates $h(PWD_{MNnew} \oplus R_{MNnew} \oplus F)$, $V_{MNnew} = K_{MN} \oplus h(ID_{MN} \| h(PWD_{MNnew} \oplus R_{MNnew} \oplus F))$ where $K_{MN} = V_{MN} \oplus h(ID_{MN} \| h(PWD_{MN} \oplus R_{MN} \oplus F))$. The MN replaces V_{MN} with V_{MNnew} and finally smart card comprises $\{V_{MNnew}, H_{MN}, SID_{MN}, h(.), R_{MNnew}, F\}$.

D. Dynamic Mobility Management

The MN during movement can be either in its home network or foreign network. It is assumed that MN changes its attachment from previous CMA (*p*CMA) to new CMA (*n*CMA) at foreign network, the *n*CMA first tries to get the MN's HoA/HNP configuration status from its home network. Then, it updates the new routing location of MN (i.e. IP address of *n*CMA). When MN is attached to *n*CMA, the new HoA/HNP is assigned to MN which is anchored at *n*CMA. Both the new and the old HoA/HNPs' are accessible for the MN. Among these, the new HoA/HNP is preferred as source IP by the new initiated session, whereas the previous session can still uses old HoA/HNP as source IP for seamless session continuity. The MN has an ability to deal with multiple HoAs/HNPs [15].

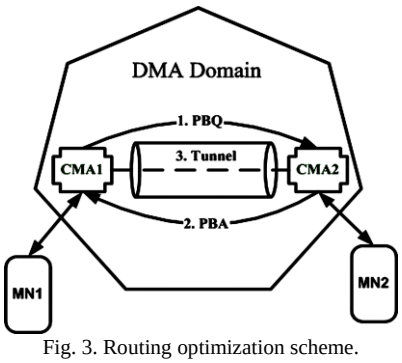

Fig. 3. Routing optimization scheme.

E. Optimized Routing

The routing optimization scheme in SIDP is shown in Figs. 3 and 4 to obtain distributing traffic volume. In Fig. 3, we assumed that the MN1 and MN2 are attached to CMA1 and CMA2 respectively. Using our optimization mechanism the MNs' would be able to communicate directly. The new mobility messages such as Proxy Binding Query (PBQ) and Proxy Binding Acknowledgement (PBA) defined in [14] are reused. When CMA1 receives packets form MN1, it will check its BCE about the HoA-to- PCoA mapping of MN2 whether it is located locally. If it does not have the routing location information of MN2, it will start buffering the packets to prevent the packet loss. The CMA1 inquires the PCoA of MN2 by sending Proxy Binding Query (PBQ) message to CMA2. CMA2 determines the HoA-to-PCoA mapping of MN2 in its BCE, and sends PBA to CMA1 because MN2 is attached to CMA2. After getting the location information of MN, CMA1 establishes tunnel with CMA2 to relays the buffered packets in order to deliver it to MN2.

Further, in Fig. 4 we assumed that MN2 is attached to CMA3, and CMA2 is supposed to be an anchor for optimized routing. The CMA1 determines the location information of MN2 after getting packets from MN1. If it does not have, it forwards the traffic to CMA2 based on the assumption using regular IPv6 routing mechanism. The CMA2 checks its BCE whether it has the HoA-to- PCoA mapping of MN2 locally. If not, it starts buffering the packets and inquires about PCoA of MN2 by sending PBQ message to CMA3. In response, the PBA is sent to CMA2 by CMA3 which includes the HoA-to-PCoA mapping of MN2. The CMA2 forwards the buffered packets to CMA3 and in parallel sends the redirect message to CMA1 about the location information of MN2. The CMA1 upon obtaining the HoA-to- PCoA mapping of MN2, establishes tunnel with CMA3 to deliver the rest of the traffic to MN2 through CMA3.

In the case when MN2 is attached to CMA1, the CMA1 first checks its BCE for HoA-to- PCoA mapping of MN2. If it has, it starts forwarding the traffic to MN2 and thus routing is handled locally.

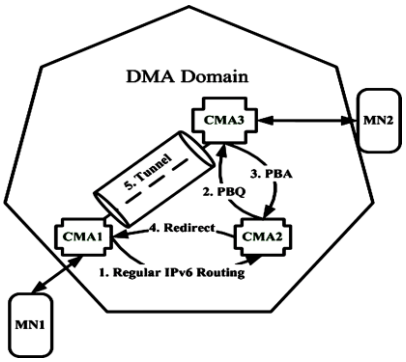

Fig. 4. Assumption of CMA2 as an anchor for optimized routing.

F. Handover

The inter-domain handover process of our proposed scheme is shown in Fig. 5, whereas the signaling flow from Anchor-Domain (A-Domain) to Serving-Domain(S-Domain) is demonstrated in Fig. 6. The entities with alphabet A and S in Fig. 6 mean that these belong to A-Domain and S-Domain respectively, such as A-CMA2, S-CMA1, etc. While performing handover from one domain to another, the MN sends deregistration message to A-CMA2 in Step 1. Subsequently, A-CMA2 manages the PBU and PBA messages locally because of the inclusion of both MAG and control panel functionalities in CMA. The deregistration message is forwarded to A-DMA by A-CMA2 in Step 3. After getting HoA-to-PCoA mapping de-registration message, the A-DMA sets D flag to 1 and starts buffering the packets on temporary basis in step 4 to avoid the packet loss. Moreover, the A-DMA waits for obtaining MN's new HoA-to-PCoA mapping registration message.

We adopt predictive approach to exchange the required information between CMAs of A and S domains before the attachment of MN to S-CMA1. In Step 5, the A-CMA2 sends the proxy handover initial (proxy HI) message having MN's

profile to S-CMA1. The S-CMA1 checks the legality of A-CMA2 and sends proxy handover acknowledgement (proxy HAck) to A-CMA2 in step 6. The MN sends attachment and login request to S-CMA1 after successful exchange of HI/Hack messages. S-CMA2 allocates S-DMA3, assigns HNP and setup BCE for MN. The registration message of HoA-to-PCoA mapping for MN with 'D' flag set to zero is sent to S-DMA3. Subsequently, S-DMA3 sends Proxy Binding Update (PBU) message to A-DMA2 in order to update the current location of MN. The A-DMA1 upon receiving new HoA-to-PCoA mapping information of MN, sends Proxy Binding Acknowledgment (PBA) message, establishes the tunnel, and forward packets to S-DMA3. In parallel of Steps 10 and 11, the tunnel is established between S-CMA1 and S-DMA3, over which route is setup for home network prefix of MN. The S-CMA1 then sends route advertisement (RtrAdv) to MN. After getting PBA from A-DMA2 and packets through tunnel the S-DMA3 starts forwarding the packets to S-CMA1. The S-CMA1 delivers the packets to MN, and following new optimized route is to be used for communication between MN and CN.

CN2 → S-DMA3 → S-CMA1 → MN

Notice that the flow of registration messages probably arrive before the flow of de-registration messages.

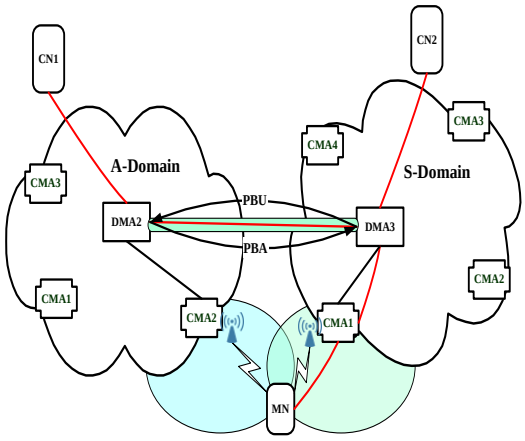

Fig. 5. Inter-domain handover process for SIDP.

IV. Security Analysis

The security analysis of SIDP is discussed in this section. A collision free one-way hash function is used through which $h(y)$ of the value y can be directly calculated. But, it is hard to obtain y from given value of $h(y)$ and it also acquires a high computational cost. Hence, getting the value of y is computationally infeasible for the intruder. Additionally, we equip our proposed scheme with password, random nonce, and fingerprint to toughen its security. The following properties prove the security strength of SIDP.

A. User Anonymity

The SIDP offers user anonymity by using symmetric cryptographic and hash operations. In the registration phase the real identity of the MN is submitted to CMA using a secure channel. The CMA decrypts $SID_{MN} = (ID_{CMA} \oplus ID_{MN})$ X_{CMA} and keeps the real identity of MN. Thus, an adversary cannot obtain the identity of MN.

B. One-Time Session Key Agreement

In SIDP, only one round trip is required to generate the session key between MN-CMA, CMA-CMA, and CMA-DMA. The confidentiality is maintained using a hash function and random nonce to encrypt the subsequent packets. In order to make session key capable against replay attacks, we used different random nonce for each session. Hence, even if an adversary captures the message, it will be hard to derive or guess session key.

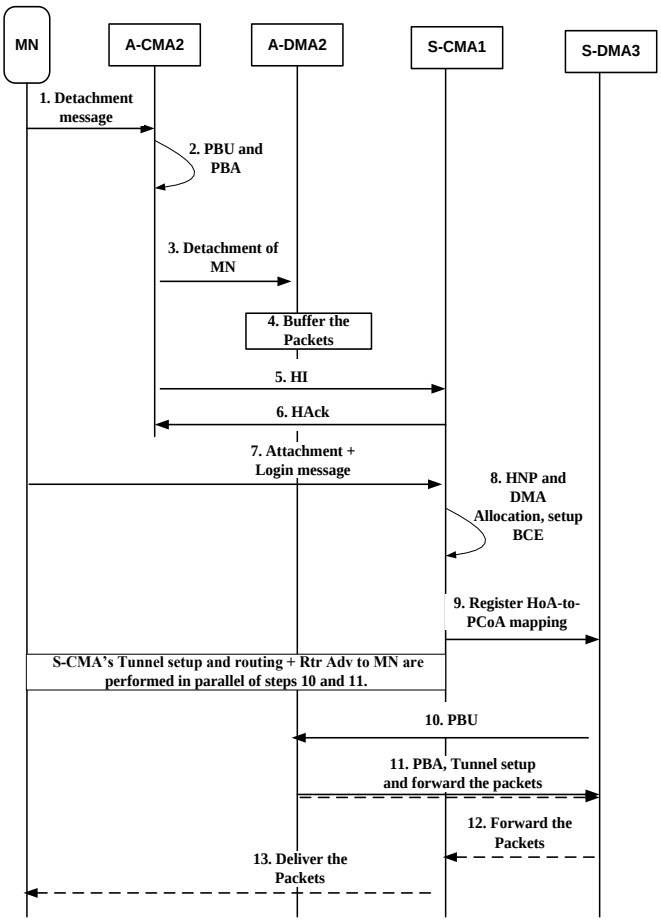

Fig. 6. Signaling flow for the SIDP handover process.

C. Mutual Authentication

In SIDP, the mutual authentication among entities is performed such as MN can verify the legality of CMA, and CMA can guarantee whether MN is valid. In the same way, two CMAs or between CMA and DMA mutual authentication could be achieved. Assuming M_1 is captured by an adversary and makes an attempt to forge a MN valid message. The MN must generate a valid message to CMA in order to make the forgery successful. But, it is hard for the adversary to calculate valid message because TK_{MN} and the random nonce n_0 is unknown to adversary. Hence, CMA stops the authentication by declaring the adversary illegal.

D. Fraud Avoidance

In SIDP, the fraud is avoided through mutual authentication, for which first the validity of each entity is checked, then session key is created for further communication. If, an adversary performs impersonation attack to cheat any entity, it cannot be achieved successfully

because it will be declared illegal during validation. Suppose an adversary impersonates MN to cheat CMA by sending fake ID_{MN} and secret key K_{MN}. The fraud will be detected by CMA as soon it encrypts E^*. It is because the adversary does not have information about real identity of MN and CMA cannot obtain $\{h(ID^*_{MN}), ID^*_{CMA}, n_0\}$. Additionally, the secret keys are protected through collision free one-way hash function $h(.)$, which makes it hard for an adversary to perform impersonation attack and can cheat any entity.

E. Forward Secrecy

The forward secrecy ensures that the passive adversary may not be able to derive succeeding session keys without having information about subset of keys. Our proposed scheme has $h(K_{MN})$ for each session and it is remained fixed. We assume that adversary has information about sk_j and sk_{j-1}, it may be able to obtain n_{j-1} by decrypting the message (n_{j-1} || $PCert_{MN}$ ||Additional information) sk_{j-1}. Hence, an adversary may try to compute $h(K_{MN})$ from $sk_j = h(h(K_{MN}))$. But, it is hard to derive $h(K_{MN})$ because the sk_j can be obtained through $h(.)$. The information about n_{j-1} still cannot help an adversary to achieve $h(K_{MN})$. Additionally, the $sk_{j+1}(= h(h(K_{MN}) || n_j))$ cannot be computed by an adversary without knowing about $h(K_{MN})$. Thus, our proposed scheme has the ability to insure forward secrecy in real sense.

F. Backward Secrecy

The backward secrecy guarantees that an inactive adversary may not be capable to obtain the preceding session keys without knowing about subset of keys. The $h(K_{MN})$ is fixed for each session in our proposed scheme. We assume that adversary has knowledge about sk_{j+1} and sk_j, it can obtain n_j by decrypting message (n_j || $PCert_{MN}$ || *Additional information*) sk_j. But, the derivation of $h(K_{MN})$ is quite hard because sk_j can be obtain using $h(.)$. If the information about $\{n_j, n_{j+1}\}$ is known to adversary, the $h(K_{MN})$ still cannot be obtain. Furthermore, the sk_j ($=h(h(K_{MN}) || n_{j-1})$) cannot be computed if the $h(K_{MN})$ is unknown to adversary. Therefore, our proposed scheme has the ability to provide backward secrecy in real manner.

V. Conclusion and Future Work

In this paper we propose a novel secure inter-domain distributed PMIPv6 (SIDP) to overcome the limitations in traditional centralized PMIPv6. The limitations are single point failure, low scalability, signaling overhead, non-optimal routing, authentication latency, and inter-domain mobility support. The SIDP defines two new mobility anchors called Control Mobility Anchor and Data Mobility Anchor by splitting the traditional mobility anchors. In CMA, the functionalities of mobile access gateway (MAG) and control plane are combined whereas, in DMA the data plane packets are buffered and forwarded. There can be multiple CMA and DMA in order to accommodate large number of mobile nodes. Further, our proposed scheme is equipped with strong authentication procedure which can be easily implemented in mobile devices due to symmetric cryptographic and collision free one way hash function.

In future, the proposed scheme will be analyzed in terms of handover latency, handover blocking probability, packet loss, and its numerical results will be obtained.

References

[1] H. Luo, H. Zhang, Y. Qin, and V. C. Leung, "An Approach for building scalable proxy mobile IPv6 domains," *IEEE Transactions on Network and Service Management*, vol. 8, no. 3, pp. 176-189, 2011.

[2] H. Tuncer, A. Kwasinski, and N. Shenoy, "Performance analysis of virtual mobility domain scheme vs. IPv6 mobility protocols," *Computer Networks*, vol. 57, no. 13, pp. 2578-2596, 2013.

[3] N. Tien-Thinh and C. Bonnet, "DMM-based inter-domain mobility support for Proxy Mobile IPv6," in *Proc. 2013 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2013, pp.1998-2003.

[4] G. Giaratta, "Interactions between proxy mobile IPv6 (PMIPv6) and mobile IPv6 (MIPv6): Scenarios and related issues," *RFC 6612*, May 2012.

[5] N. Neumann, J. Lei, X. Fu, and G. Zhang, "I-PMIP: An inter-domain mobility extension for proxy-mobile IP," presented at IWCMC, June 2009.

[6] J. C. Zuniga, C. J. Bernardos, A. de la Oliva, T. Melia, R. Costa, and A. Reznik, "Distributed mobility management: A standards landscape," *IEEE Communications Magazine*, vol. 51, no. 3, pp. 80-87, 2013.

[7] I. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 16-28, 2004

[8] Z. Ma, K. Wang, and F. Zhang, "Network-based inter-domain handover support for PMIPv6," *Internet-Draft*, January 2012.

[9] T.-X. Do and Y. Kim, "Network mobility support in the distributed mobility management," *Internet-Draft*, October 2013.

[10] D. H. Shin, D. Moses, M.Venkatachalam, and S. Bagchi, "Distributed mobility management for efficient video delivery over all-IP mobile networks: Competing approaches," *Network, IEEE*, vol. 27, no. 2, pp.28-33, 2013.

[11] D. Liu, J. Song, and W. Luo, "PMIP based distributed mobility management approach," *IETF Draft*, draft-liu-dmm-pmip-based-approach-00, July 3, 2011.

[12] S. Koh, J. Kim, H. Jung, and Y. Han, "Use of proxy mobile IPv6 for distributed mobility control," *IETF Draft*, draft-sjkoh-mext-pmip-dmc-03, June 30, 2011.

[13] C. J. Bernardos, A. de la Oliva, F. Giust and T. Melia, " A PMIPv6-based solution for distributed mobility management," *IETF draft*, draft-bernardos-mext-dmm-pmip-01, July 11, 2011.

[14] W. Luo and S. Tricci, "Distributed mobility management approach with mobile IP and proxy mobile IP," *IETF*, draft-luo-dmm-with-mip-and-pmip-00, October 15, 2012.

[15] L. Yi, H. Zhou, and H. Zhang, "An efficient distributed mobility management scheme based on PMIPv6," in *Proc. 2012 IEEE Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2012, pp. 274-279.

[16] W. Diffie and M. E.Hellman, "New directions in cryptography," *IEEE Transaction on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

Muhammad Zubair has done his bachelor and master degrees in Computer Science from University of Peshawar, Pakistan in 2005 and 2007 respectively. Currently, he is a PhD student at Dalian University of Technology (DUT), Dalian, China. He is also member of Doctor Association in School of Information and Communication Engineering, DUT. His research interest lies in wireless communication system; particularly focusing on topics related to all aspects of mobility, QoS and security in Next Generation Networks.

Xiangwei Kong is currently a professor and director of Research Center of Multimedia Information Processing and Security of Dalian University of Technology, China. During 2006–2007, she was a visiting scholar of Purdue University, USA. Prof. Kong is a member of signal processing society of IEEE. From 2004–2009, she is a vice director of multimedia information security branch of Chinese Institute of Electronics, China. Her research contributions encompass aspects of multimedia information security, digital watermarking, digital image forensics, image and signal processing, and wireless networks.

Saeed Mahfooz has done his Ph.D. from Liverpool John Moore University, Liverpool, UK in Distributed Multimedia Systems in 2001. He started his teaching career in 1990 which spans around 22 years. He is also heading the Computer Networks Research Group at Department of Computer Science, University of Peshawar. His research interest includes QoS Architectures, QoS Routing, Network Protocols, IPv6, Cloud Computing, Wireless Networks, MANETs, future Internet architecture and Next Generation Networks.

Irum Jamshed has done her bachelor's degree in Information Technology from University of Peshawar in 2008. She has completed her MS-IT from Institute of Management Sciences (I|MS), Peshawar in 2011. Currently she is data manager in IRC KP - Pakistan. Her research interest is related to wireless communication covering different areas including QoS, mobility and security.