Secure Communication Channel Architecture for Software Defined Mobile Networks

INTRODUCTION

* Software- Defined Networking (SDN) : Offers three new features

logically centralized intelligence,

programmability

abstraction

using inexpensive hardware

* Network Function Virtualization (NFV) : Allows decoupling the network functions from proprietary hardware appliances, so they can run in software.
* These features enhance flexibility, scalability and performance of mobile networks
* However, added SDMN features such as centralized controlling, network programmability and network function virtualization introduce new security challenges to mobile networks
* Therefore, the security of SDMN is still an open issue and it is a timely research topic to discuss.

SDMN and its security issues

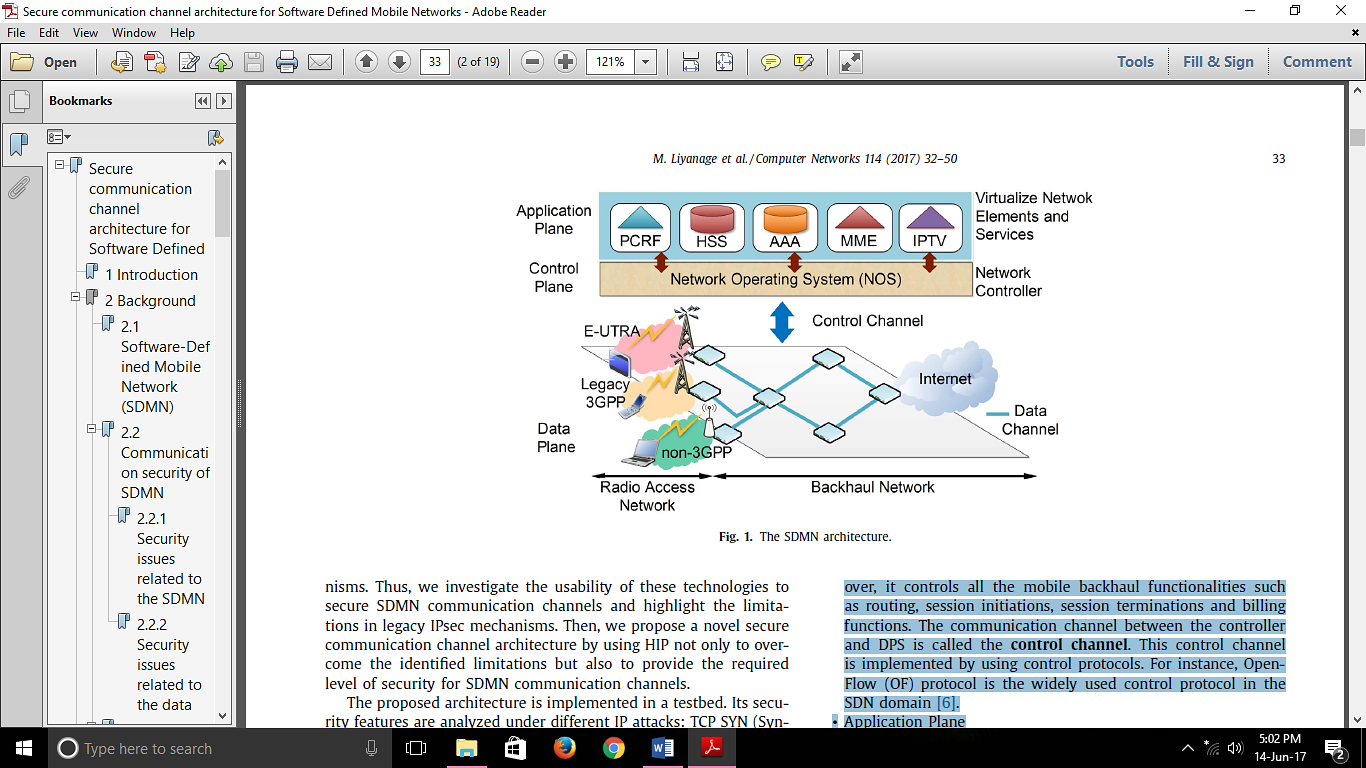
1. Software-defined Mobile Network ( SDMN )

Contains three plains :

* Data Plane (DP)
* SDN concepts separate control plane from data plane of network.
* Pushes network intelligence to a centralized controller.
* DP now consists of low-end switches and network links among them.
* Base stations, wireless access points and Internet are connected to these DP switches (DPSs).
* User traffic is transported through the data plane.
* This communication channel is called the **data channel** .
* Control Plane (CP)
* Consists of a logically centralized controller which provides the consolidated control functionalities.
* The centralized controller supervises packet forwarding functions of network through an open interface.
* It controls all the mobile backhaul functionalities such as routing, session initiations, session terminations and billing functions.
* Communication channel between the controller and DPS is called the **control channel** .
* This control channel is implemented by using control protocols.
* For instance, Open- Flow (OF) protocol is the widely used control protocol in the SDN domain
* Application Plane
  + Consists of end-user business applications and other control entities.
  + Legacy mobile network control devices such as
  + Policy and Charging Rules Function (PCRF),
  + Home Subscriber Server (HSS),
  + Mobility Management Entity (MME)
  + Authentication Authorization and Accounting (AAA)

are now software applications which are running on top of the Network Operating System (NOS) at the application plane.

* + Boundary between application and control layers is traversed by northbound API.



1. Communication security of SDMN

Two types of communication security :

(1) Security issues related to the control channel

(2) Security issues related to the data channel

1. Security issues related to the control channel

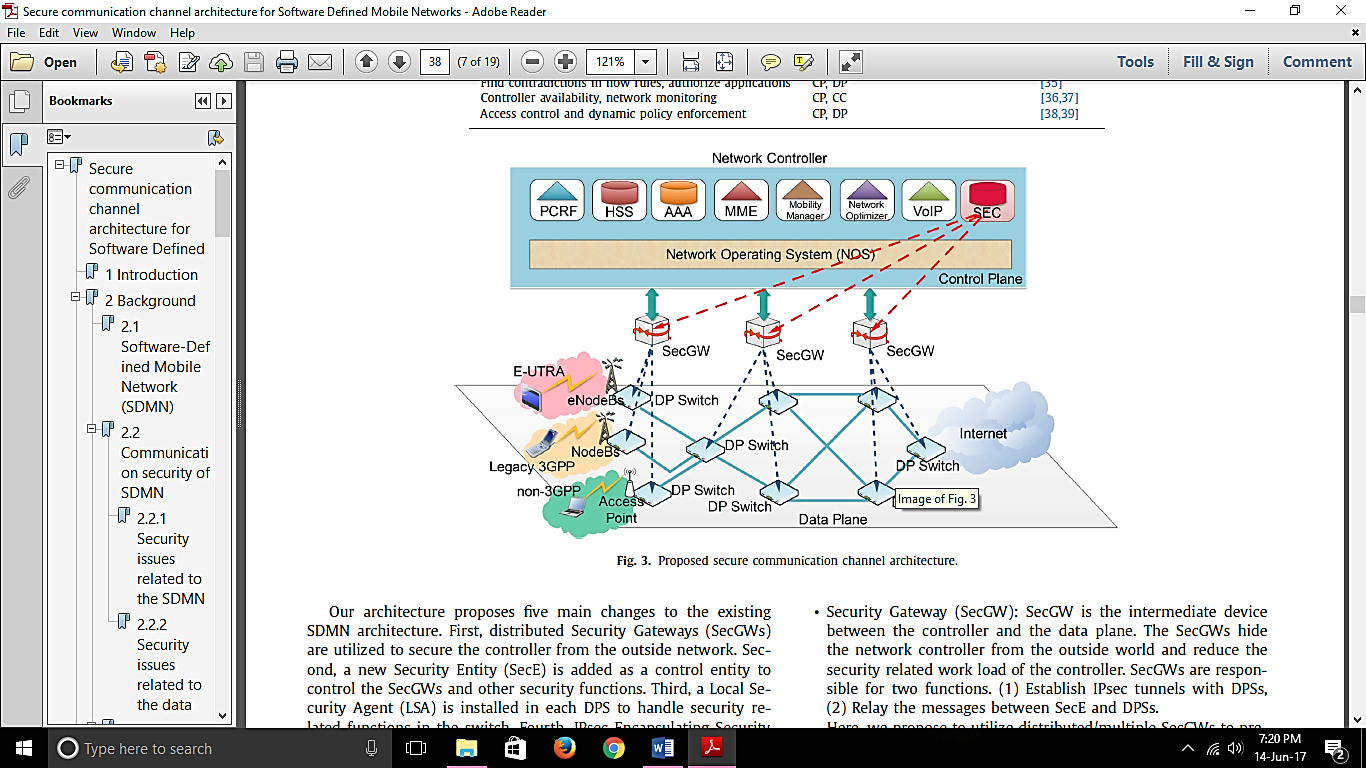
* Lack of IP level security
* Existing SDMN control protocols rely on higher layer secure mechanism such as TLS
* Higher-layer secure mechanisms are vulnerable to IP based attacks such as IP spoofing, TCP SYN, DoS and TCP reset attacks
* Higher layer protection mechanisms are not enough to provide required level of robustness and security for the control channel
* Strong authentication mechanism required between the controller and DPSs
* Intruders can impersonate as legitimate DPS and launch security attacks on the control channel
* TLS/SSL sessions do not utilize a strong authentication procedure between controllers and switches
* Attacks on the network controller
* Security of the control channel is a key factor to ensure the proper communication with the controller

1. Security issues related to the data channel

* SDN Scanner attacks
* Current SDMN backhaul traffic is unencrypted
* Attackers can perform “SDN Scanner” mechanisms to collect network information.
* Later, this information can be used to perform IP based attacks such as DoS, reset, replay and spoofing attacks
* Flow modification attack
* Current SDMN data channel does not contain any integrity protection mechanism.
* Attacker can alter or destroy the data without being noticed by the network operator.
* The alternations of data flows may result to decrease the Quality of Service (QoS) of communication sessions
* Requires strong mutual authentication mechanisms for the data channel as well
* Intruders can impersonate as legitimate switches and inject forged traffic flows to the data plane.
* Attacker can exhaust the flow tables of DPS and reduce the available bandwidth for user traffic.
* It will also affect the control plane by inducing unnecessary flow requests to the controller

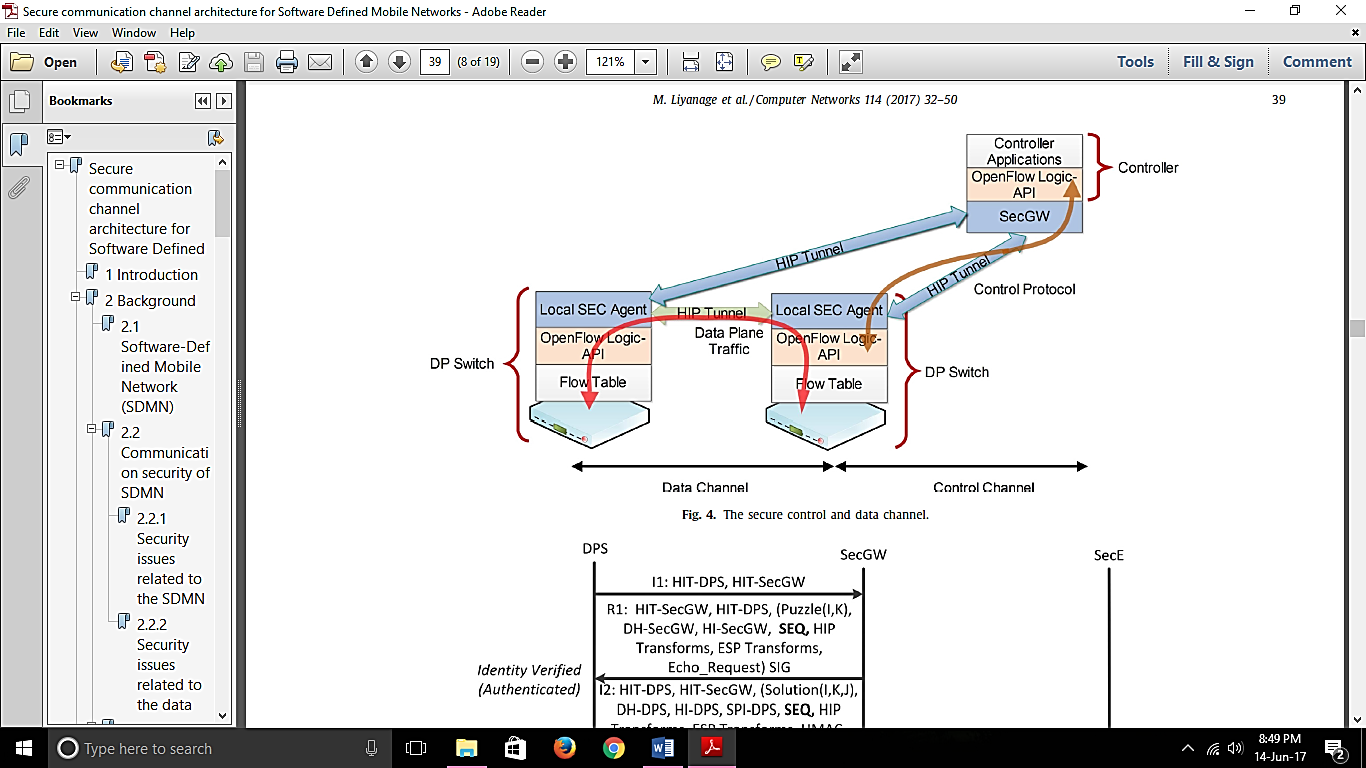
Proposed secure communication channel architecture

* A novel IPsec based SDMN backhaul traffic architecture to secure the communication channels.
* It is a “bump-in-the- wire” security architecture based on HIP
  + *Host Identity Protocol (HIP) :*
    - HIP is a novel mobility and security management protocol which is standardized by IETF.
    - HIP separates the dual role of IP address as the locater and the host identity.
    - Each HIP host has a public/private key pair and the public key is used as its Host Identity (HI).
    - HIP utilizes a base protocol - HIP Base Exchange (HIP BEX) to mutually authenticate the end nodes.
    - HIP establishes a Security Association (SA) for IPsec tunnels.



Five main changes to the existing SDMN architecture:

* Distributed Security Gateways (SecGWs)
  + Utilized to secure the controller from the outside network.
  + Intermediate device between the controller and the data plane.
  + Hides the network controller from the outside world and reduce the security related work load of the controller.
  + Responsible for two functions:
    - Establish IPsec tunnels with DPSs,
    - Relay the messages between SecE and DPSs.
  + Here, utilize distributed/multiple SecGWs to prevent a single point of failure.
  + It is possible to integrate various security functions such as Intrusion Detection Systems (IDS), Deep Packet Inspection (DPI) and Firewalls within SecGWs to provide extra protection.
* Security Entity (SecE)
  + Added as a control entity to control the SecGWs and other security functions.
  + New control entity which controls the SecGWs and other security functions.
  + Authorizes DPSs based on Access Control Lists (ACLs).
  + The network operator uploads a set of ACLs which contain the identities of legitimate DPSs.
  + Also generates Traffic Encryption Keys (TEKs) for both control and data channels.
  + Cooperates with other control entities (e.g. Traffic Optimizer Entity (TOE)) to manage the tunnel establishments in the control and data channels.
* Local Se- curity Agent (LSA)
  + Installed in each DPS to handle security related functions in the switch
  + Local SEC Agent (LSA) LSA is a security entity which is implemented in each DPS.
  + Mainly responsible for HIP tunnel establishments with SecGWs and other DP switches.
* IPsec Encapsulating Security Payload (ESP) Bounded-End-to-End-Tunnel (BEET) mode tunnels
  + Used to secure the control and data channels communication.
* Session based Traffic Encryption Keys (TEKs)
  + Used to encrypt the control and data channel traffic.
  + The proposed architecture uses three types of TEKs:
    - * Control Traffic Encryption Key (CTEK)
        + Used to encrypt the control channel traffic.
        + SecE periodically generates CTEKs and distributes them to the DPSs.
        + CTEKs are encrypted by using KEK of DPS and delivered via SecGWs.
      * Data Traffic Encryption Key (DTEK)
        + Used to encrypt the data channel traffic.
        + SecE periodically generates DTEKs and distributes them to the DPSs.
        + DTEKs are also encrypted by using the KEK of the DPS and delivered via the SecGWs.
      * Key Encryption Key (KEK)
        + Used to encrypt CTEKs and DTEKs during the delivery via the secure control channel.
        + The KEK is unique to each DPS.
        + SecGW and each DPS agreed on this KEK during the tunnel establishment procedure by using Diffie-Hellman (D-H) key exchange protocol.
        + KEKs are periodically updated by using D-H key exchange protocol.



HIP based control channel

* A HIP (IPsec ESP BEET mode) tunnel is established between SecGW and LSA.
* The controller and DPSs can communicate by using the traditional control protocol without any modification.
* The proposed security mechanism is invisible to the existing control protocol.
* *Authentication and registration procedure of DPSs :*
  + - Proposed architecture supports the dynamic addition of new DPSs and the automatic control channel establishment.
    - A novel tunnel establishment procedure based on HIP BEX. It supports two tasks :
      * Authenticate and register a new DPS.
      * Establish an IPsec (ESP BEET mode) tunnel between the DPS and SecGW.
* Every DPS has its own public/private key pair.
* Public key is used as its host identity (HI).
* Public/private key pair is stored in each DPS before the installation in the network.
* At the same time, the network operator adds the HIs of the legitimate switches to the ACLs.
* To be able to register to the network, the DPS should be aware of the HI of the SecGW to which it wants to register.

Steps

1. DPS initiates tunnel establishment procedure by sending **an I1 message**.

It contains the HITs (Host Identity Tags) of DPS and SecGW.

*HIT corresponds with the 128-bit hash of the HI.*

1. To prevent DoS attacks, SecGW replies the I1 message with a pre-computed **R1 message** without allocating any resources

*Components of the R1 message:*

* *cryptographic puzzle,*
* *D-H key parameters,*
* *public key of SecGW,*
* *ESP transforms,*
* *HIP transforms,*
* *echo request*
* *signature*

1. DPS sends the I2 message.

*Components of the I2 message:*

* *HMAC (Hash Message Authenti- cation Code),*
* *solution of the cryptographic puzzle,*
* *D-H key parameters,*
* *public key of the DPS, SPIs,*
* *ESP transforms,*
* *HIP transforms*
* *signature.*

1. SecGW sends the switch’s credentials to SecE via REQ message. It contains

* HIs of DPS and SecGW,
* authentication request,
* echo request.

1. Upon the arrival of REQ, SecE checks the received HIs against the ACLs and the network optimizer.

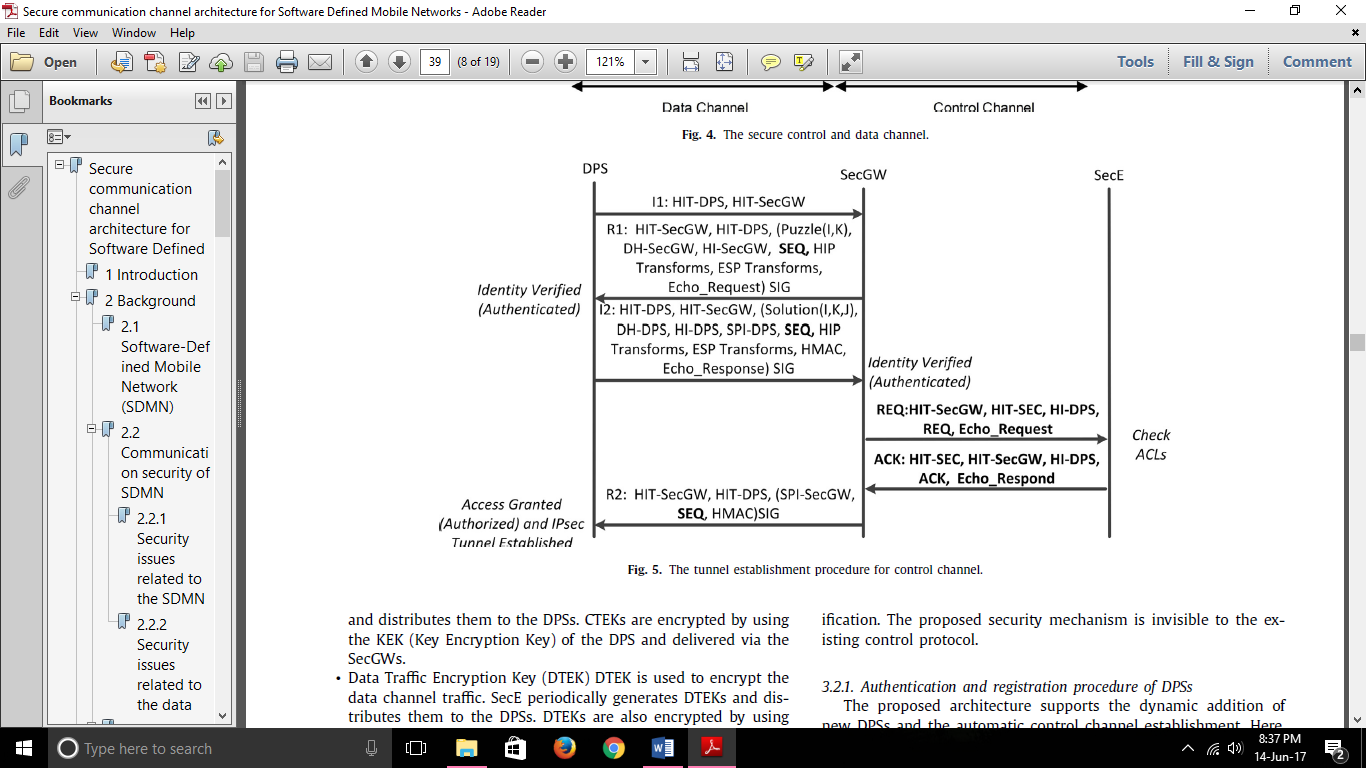
Then, it replies the REQ message with an ACK message. The ACK message contains

* two HIs,
* the acknowledgment
* the echo reply.

*Here, the HI of the DPS is checked with the ACLs by SecE. This step prevents unauthorized access to the network.* Moreover, SecE keeps a record of the different requests with a time stamp. It helps to identify replay attacks. If a DPS sends premature requests again and again, those requests will be dropped.

1. TOE checks the HIs of DPS and SecGW with the traffic optimization procedure.

*(A positive acknowledgment is sent for a request from an authorized DPS and a negative acknowledgment is sent for other re- quests. In case of a negative acknowledgment, SecGW drops the connection request from the DPS. Otherwise, SecGW completes the tunnel establishment by sending the R2 message. It contains the HIs of DPS and SecGW, SPIs, HMAC and the signature.)*

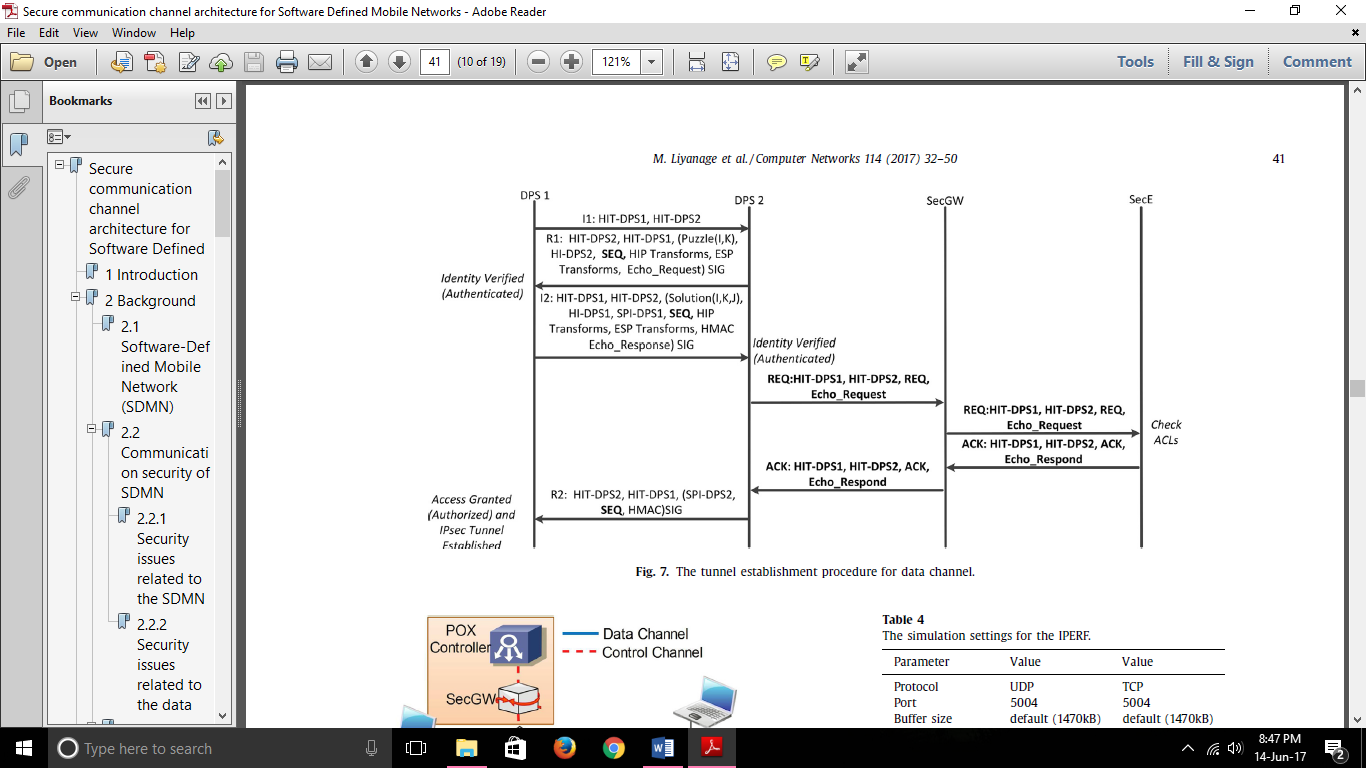


HIP based data channel

* HIP tunnels are established between LSAs to secure the data channel.
* The proposed security mechanism is invisible to the DP traffic.
* Thus, the traditional DP traffic is transported between DPSs without any modification.
* *Three changes to the existing SDMN data channel:*
  + DPSs are mutually authenticated based on a PKI mechanism before any data exchange.
  + Communication session establishment between DPSs is authorized based on ACLs and other control entities (e.g. TOE).
  + IPsec (ESP BEET mode) tunnels are established between switches to secure the data channel communication.
* *Tunnel establishment procedure of data channel:*
  + Tunnel establishment procedure is almost like the tunnel establishment procedure of the control channel.
  + Steps

1. I1, R1, I2 and R2 messages have the same obligatory field as in the previous control channel tunnel establishment
2. But DPS2 sends the REQ message to SecE via SecGW. It contains the HIs of DPSs and the echo request.
3. Upon the arrival of REQ, SecE checks the received HIs with ACLs and TOE.
4. Then, it replies the REQ message with an ACK message. The ACK message contains the HIs of the DPSs, the acknowledgment and the echo reply.

*(A positive acknowledgment is sent for a request from authorized DPSs and a negative acknowledgment is sent for other re- quests. If it is a negative acknowledgment, DPS2 drops the connection request from DPS1. Otherwise, DPS2 completes the tunnel establishment by sending the R2 message.)*



Conclusion

* Proposed architecture protects the communication channels against IP based attacks such as DoS, reset, spoofing, replay and eavesdropping attacks.
* However, there is a performance penalty of security on throughput, latency and jitter due to the extra IPsec tunnel establishment.
* This drawback can be minimized by using security specific hardware and maintaining established HIP tunnels for a longer period.

Link: [..\sec protcols\2017 = 1-s2.0-S1389128617300075-main.pdf](../sec%20protcols/2017%20=%201-s2.0-S1389128617300075-main.pdf)