Architecture for Satellite Services over Cryptographically Heterogeneous Networks with Application into Smart Grid

Vahid Heydari Fami Tafreshi
Centre for Communication Systems Research (CCSR) University of Surrey
Guildford, United Kingdom
v.fami@surrey.ac.uk

Haitham Cruickshank
Centre for Communication Systems Research (CCSR) University of Surrey
Guildford, United Kingdom
h.cruickshank@surrey.ac.uk

Zhili Sun
Centre for Communication Systems Research (CCSR) University of Surrey
Guildford, United Kingdom
z.sun@surrey.ac.uk

Abstract— The rapid growth in the demand for Future Internet services with many emerging group applications has driven the development of satellite, which is the preferred delivery mechanism due to its wide area coverage, multicasting capability and speed to deliver affordable future services. Nevertheless, security has been one of the obstacles for both satellite services as well as smart grid group applications, especially with logical/geographical/cryptographic domains spanning heterogeneous networks and regions. In this paper, adaptive security architecture is implemented to protect satellite services for smart grid group applications. The focus is on key management and policy provisioning. Leveraging Group Domain of Interpretation (GDOI) as the standard for smart grid centralized key/policy management architecture, a single Domain of Interpretation (DOI) is deployed and evaluated critically in terms of the added protocol signaling overhead on the satellite system for a fixed-network scenario. This also partially realizes the growing trend towards the use of TCP/IP technology for smart grid applications.

Keywords—satellite systems; secure group communications; policy; key management; smart grid; GDOI

I. INTRODUCTION

As an integral part of the Future Internet, satellites and their broadcast characteristics can be utilized to provide an economical wide-area multicast service. On the other hand, group-oriented applications with multicasting capacity are progressively deployed more and more at the Internet scale. Developing any-to-any distributed applications in essence is preferred with multicast development [1]. Smart grid applications for instance, require secure multicast communication covering large geographical areas and hence satellite networking is ideal for providing such connectivity especially for rural or difficult locations. However, security for the group-oriented applications in which a group spans multiple logical/geographical/cryptographic domains remains the Achilles heel.

Our previous work in [2] detailed three different scenarios, namely mobile-network scenario for the applications such as mobile broadband, fixed-network scenario with smart grid applications and finally Delay Tolerant Network (DTN) scenario with deep-space application; and a scalable and adaptable security architecture was proposed to ensure the security of satellite services. Nevertheless, as [2] reflects as the future direction, a secure group management protocol needs to be implemented/critically evaluated amongst all the involving entities such as senders/receivers and key/policy managers. In this work, we aim to clarify security ambiguities regarding key/policy management protocol over unicast/multicast conduits with empirical studies. Our practical studies here provide sufficient support to the previously presented approach by demarcating how a centralized architecture with secure key/policy management in the fixed-network scenario with smart grid application is deployed/evaluated in practice.

For this, section II discusses how smart grid and satellite networking complement each other. Section III overviews the security obstacles along the way and shows the direction of this work to remove them. Section IV then introduces our fixed-network smart grid architecture with satellite and more importantly stresses the role of secure group management protocol within the satellite domain. Emulation scenario and its experimental results are provided in section V. Section VI critically evaluates the performance of the results in section V. Section VII draws the main conclusions and reflects on the future directions of this study.

II. SMART GRID AND SATELLITE NETWORKING

Based on [3], supervisory control and data acquisition (SCADA) in addition to the teleprotection and video surveillance are known as the three significant applications amongst smart grid established applications. By means of the former, power grid field data is acquired and transferred to the central systems for monitoring/controlling grid components/sensors. The teleprotection refers to the mechanism by which detecting a fault raises the alarm for the other end(s). Having said that, for best practice, power grid utility companies separate the control network (management platform for SCADA, teleprotection or surveillance applications) from the corporate network in the production environment (customer-related applications).

978-1-4799-5893-1/14/$31.00 ©2014 IEEE

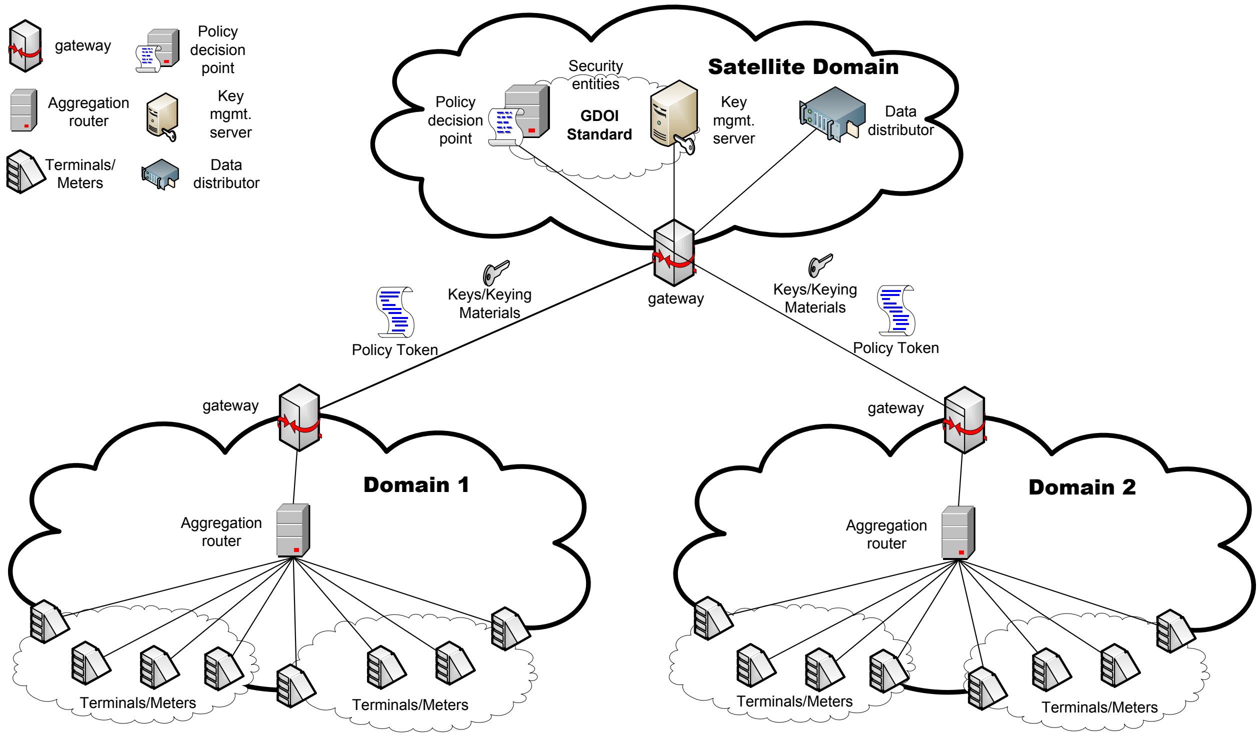


Fig. 1. Fixed-network scenario with smart grid application

Considering the rising tendency towards the use of TCP/IP technology for the smart grid, utility corporations may deploy multiple communication systems while IP remains the most common management platform. Network segmentation and traffic separation are generally performed herein with the aid of virtual private networks (VPNs) [3]. Hence remote access through external networks is required to be encrypted and access-list protected exploiting IPsec [4] and group-based encryption. In terms of large geographical areas, smart grid needs secure multicast means of communication with widespread coverage. Satellites are therefore an ideal solution for communications amongst remote substations within the smart grid infrastructure.

In addition to the widespread coverage over the remote substations (placed in difficult locations for instance), satellite becomes a viable option for different smart grid applications since [5]:

- Robust security is crucial for smart grids. Provisioning broadband services by satellites to remote substations gives rise to the development of security related applications such as video surveillance or teleprotection.
- Satellite backs up terrestrial communications for critical grid infrastructure and provides redundancy.
- For emergency response for disaster recovery, satellite ensures business connectivity for the smart grid.
- For areas ill-served by the Internet technologies, enhanced metering infrastructure can benefit from satellites by backhauling from meter aggregation gateways.
- Satellites can address monitoring/controlling requirements for the smart grids and perform distribution nodes management.

It is noteworthy that the definition of remote sites within smart grid is not merely limited to the locations which are geographically spread over far areas. Sites can be economically remote (and thus satellite services are essential) whereby installation costs for alternative solutions are high or their deployments are unfeasible (due to the interference issues, site restrictions or their logically/cryptographically heterogeneous nature for example).

III. Security Issues and Objectives

It should be noted that our work needs to think through security challenges inherent to both satellite services as well as smart grids conjointly. Firstly, the applicability of remedies for the smart grid in terms of communication mechanisms and its overall security still remains an open challenge [6]. Smart grid distribution networks based on the communication type are susceptible to different threats including passive/active eavesdropping, protocol failures, DoS or man-in-the-middle attacks and thus enhancing the cyber security of the future grid infrastructure is vital [7]. Parallel to security, privacy of the information metered is another challenging issue in the smart grids [8]. [9] stresses that by sending fake commands to smart meters or a group of them in a region by an adversary, human life can be

978-1-4799-5893-1/14/$31.00 ©2014 IEEE

threatened through stopping power delivery or invalid switching of electric devices.

On the other hand, active threats such as masquerading or Denial-of-Service (DoS) against the security of satellite services are more difficult for implementation than the passive threats. However, because of the broadcast nature of satellites, eavesdropping and traffic analysis are deemed to be the major passive threats for different satellite applications [10]. To thwart such passive threats, we later reveal how incorporating the security mechanisms within the satellite domain provides the ability for centralized key management and policy generation and eliminates the associated eavesdropping risks.

Considering [2, 3, 5, 9, 11, 12], we summarize the major challenges in the secure satellite services with smart grid applications as follows:

- Implementing IPsec for satellite networking; secure IP over satellite remains challenging with regard to key/policy management and traditional confidentiality, integrity and authentication security objectives. Our deployment aims to provide a secure group management platform through TCP/IP over satellite for smart grid applications.

- Communication protocols with a large number of message exchanges in the satellite systems are obstacles. Therefore, it is essential for any group management protocol in the satellite networking system to be evaluated in terms of the protocol message signaling. Too talkative protocols can end up with DoS for resource-constrained smart meter/satellite system.

- Broadcast nature of satellite networking jeopardizes the safety of the communications by leaving it at risk from eavesdropping attacks. Our results later demonstrate how eavesdropping risk is eliminated thanks to the IPsec as the heart of the secure group management protocol.

- Provisioning satellite multicast security by addressing the ambiguities pertaining to the key/policy management is difficult. Secure multicasting over satellite here is equivalent to the scoped broadcasting which targets a specific group/domain for smart grid applications.

- For a given management platform of the smart grid application, members such as meter aggregation routers can be divided logically/geographically /cryptographically into different domains/groups/sub-groups and thus group-key management is needed. The International Electrotechnical Commission (IEC) has a series of standards on substation automation within the smart grid (the automation of data acquisition and protection within substations) in which Group Domain of Interpretation (GDOI [13]) secures the distribution of domain keys while IPsec [4] ensures the IP multicast protection using these group keys (IEC 61850) [14]. That's why our emulation exploits GDOI as the secure group management protocol over satellite to effect group-based encryption which governs the centralized key/policy distribution mechanism.

IV. Fixed-network Scenario with Smart Grid

Figure 1 displays the fixed-network scenario similar to our previous work in [2]. With the fixed-network scenario whereby terminals are meter aggregation nodes with low join/leave characteristics, cryptographic goals such as confidentiality, integrity and authentication are less problematic. This additionally makes our implementation scenario herein more suitable for smart grid applications. This is because while security undoubtedly incurs costs, less dynamic groups incur less workload on the overall satellite system which is desirable. Since the workload for the group key/policy management decreases the overall performance of the satellite systems and asks for redundant energy, we later evaluate our implementation for the cryptographic group management protocol to highlight the protocol message signaling for the smart grid scenario.

The fixed-network scenario involves three domains, namely satellite domain and domains 1 & 2. Domains 1 & 2 can be logically/geographically/cryptographically separated. Terminals/meters are linked to the meter aggregation nodes which in turn aggregate data. Meter aggregation routers are connected to the external networks through gateways. While in Figure 1, domains 1 & 2 are physically separated, aggregation routers in both domains can constitute the creation of another logical domain with a different encryption/decryption algorithm or different key size (to form the management platform of the grid application like SCADA for instance). In this case, the adaptive group key management in the satellite domain is asked to provide a different set of group key/policy dynamically for the established domain. Lastly, gateway as the entry/exit point provides the connectivity to the satellite domain.

The satellite domain facilitates the centralized key management and policy provisioning through GDOI for smart grid applications. Inside the satellite domain, encrypted data with different keys for each domain is distributed with the aid of a data distributor. The different keys by which the group data inside the domain is encrypted are called Traffic Encryption Key (TEK). Each domain is also associated with a Key Encryption Key (KEK) to manage and distribute TEKs which is known as the group key common to the members of the given group/domain. The key management server facilitates KEK dissemination amongst the domains.

Policy decision point (PDP) fulfills the need of the policy server which delegates trust through generating/distributing a policy token to different domains. Policy is exploited to effect the adaptable security remedy to fluctuating security situations such as when a key is compromised. Furthermore, policy defines the re-keying conditions— an example of which is deployed later. Remember that both PDP as well as the key management server are located in the satellite domain which disseminates the keying materials and policy tokens to intended domains.

A. *Role of GDOI within the Satellite Domain*

Secure group management protocol amongst involving entities in the Figure 1 scenario such as key/policy servers, data distributors, etc. can be satisfied with either Group Secure Association Key Management Protocol (GSAKMP) [15] or GDOI [13]. Nonetheless, GDOI was standardized for the substation automation in the smart grid applications to provide secure group key distribution. GDOI also is widely considered as an encryption technology for next-generation WAN that lets trusted members of a group take advantage of a common SA (Security Association) which is independent of any endpoint IPsec tunneling relations. Whereas in traditional IPsec VPN tunnels the tunnel overlays routing (with a new IP header as the original packet) has left multicast replication inefficient, in secure group management with GDOI, highly scalable and dynamic connectivity is provisioned via IP header preservation. GDOI operates over any underlying routing infrastructure via a single unique SA shared for the entire group. Traditionally, it was O (N^2) for the number of individual SAs required for peer-to-peer IPsec tunnels which is extremely costly for satellite services.

GDOI provides a means of keying protocol for secure group management in which IPsec guarantees encryption/decryption services for data packets. In other words, secure group management lets domain routers encrypt multicast/unicast data packets removing the legacy need to fixed VPN tunnels used to protect the traffic. GDOI functions amongst a set of group members (GM) and a set of (for high availability and resiliency) group controllers/key servers (KS). ISAKMP [16] (Internet Security Association and Key Management Protocol) phase 1 SA ensures the security of GDOI communications itself. In other words, ISAKMP (more precisely Internet Key Exchange (IKE) v1 and v2 [17]) provides a secure key exchange mechanism and establishes a secure channel between GM and KS. Note that ISAKMP/IKE phase 1 SA (formed for each GM-KS pair) is different from GDOI/group SA (single and shared for the group/domain). KS is responsible for establishing SAs with group members provided that they are authorized. This mechanism allows merely the trusted members such as meter aggregation nodes or smart grid management platform components to address the group in our minds. Moreover, the KS maintains keying materials for each group along with the associated policies. Policies in addition to relevant keying materials are obtained from key servers by GMs. To put this into effect, initially a GM is required to register with a KS providing group ID to gain the group SA required to speak to the group. The registration makes authentication as well as authorization of group members possible for the KS. GM is now able to download the group IPsec policy as well as the keys needed for encrypting/decrypting multicast/unicast data over the established IKE phase 1 SA. Encrypted IP multicast packets with the aid of IPsec can be exchanged among GMs now.

GDOI adds two new ISAKMP/IKE Phase 2 exchanges namely GROUPKEY-PULL and GROUPKEY-PUSH in addition to new payload definitions to the standard ISAKMP protocol. With Pull protocol, GM contacts KS initially to retrieve group SA (representing group keying materials/policies) over the IKE Phase 1 encrypted and authenticated channel (SA) for secure group communications. On the other hand, KS initiates the Push rekey protocol exchange dispatched to the group IP multicast address (if multicast approach is chosen for the rekeying mechanism; rekeying in unicast is preferred due to the added security achieved) to deliver fresh group keying materials/policies to the authorized GMs only. This in turn might result in de-authorization of some GMs whereby they cannot participate in the secure group communications anymore (by not receiving a new rekey). New payload definitions with GDOI therefore include KEK, TEK, Group Associated Policy, Sequence Number, etc. KS listens on port 848 for GDOI Pull exchanges and might dispatch Push exchanges over the same port. In summary, with the aid of Pull exchanges, TEK and KEK are downloaded over ISAKMP/IKE phase 1 SA's protection while Push facilitates the rekeying mechanism. GM-to-GM secure communication is now provided thanks to the IPsec ESP as the data security payload.

From the architectural viewpoint, the centralized key and policy distribution mechanism with GDOI in Figure 1 allows KS to propagate keying materials as well as policies to already-authenticated GMs such as meter aggregation nodes, gateways or SCADA components to fulfill their secure site-to-site transmission goal. Centralized key management architecture benefits from ease of maintenance as well as scalable distribution for keying materials and policies.

V. System Realisation and Results

Graphical Network Simulator version 3 (GNS3) [18] has been utilized for the emulation work at this stage. GNS3 application is open source software which is free as well as platform independent and therefore available to be used with various types of operating systems including Windows, MacOS and Linux. GNS3 involves Dynamips; the core program that facilitates the Cisco IOS emulation (IOS-internetworking operating system, a software program for routing, switching, internetworking and telecommunicating of real network elements such as routers and switches). While Dynagen is the text-based front-end for Dynamips, GNS3 provides the graphical front-end for the emulation. GNS3 allows for emulation of different platforms and technologies including Cisco, Juniper, ATM, Frame Relay, etc. Besides, GSN3 emulates complex network scenarios. However, the emulator is highly memory intensive and therefore prone to systematic crashing.

The merit of this work is that GNS3 bridges between simulated parameters and the actual production environment characteristics with performing emulation rather than simulation. When satellite is in place, resource constraints are of immense significance and thus emulated analyses here are more precise and thus preferred. Particularly, minimizing signaling overhead introduced by any security mechanism and reducing the workload on the satellite system is essential. Our objectives for system realization include but are not limited to:

- Proper deployment of centralized secure group management protocol with GDOI; this should clarify ambiguities regarding the policy, IKE SA, group SA, keying/rekeying materials and conditions, and access-list protection of the remote sites/group address of the grid applications.
- Thwarting the eavesdropping risks associated with (the broadcast nature of) the satellite systems as well as smart grid applications
- Measuring the signaling overhead pertaining to GDOI placed in the satellite domain as the secure group management protocol under accurate emulation conditions utilizing flow-graph of Wireshark [19], we evaluate the signaling overhead required for each group member through GDOI to authenticate itself to the key server for the basic scenario.
- Future work aims at estimating the overhead added by data security payload with ESP as the heart of GDOI before and after cryptographic group management protocol implementation; this reveals the added workload on the satellite system for the basic scenario.

A. Implementation Scenario

Figure 2 displays the emulation topology with GNS3 for a single logical domain established upon varying heterogeneous networks. GDOI as the secure group management protocol is implemented within the satellite domain. Domains 1, 2 & 3 are geographically/physically separated over a large area.

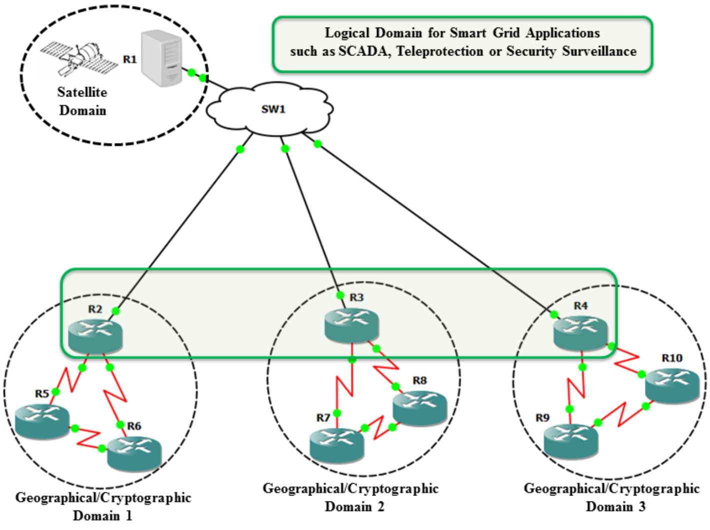

Logical Domain for Smart Grid Applications
such as SCADA, Teleprotection or Security Surveillance
R1
Satellite Domain
SW1
R2
R3
R4
R5
R6
R7
R8
R9
R10
Geographical/Cryptographic Domain 1
Geographical/Cryptographic Domain 2
Geographical/Cryptographic Domain 3

Fig. 2. Emulation scenario with GNS3, a single logical domain is chosen upon heterogeneous networks to form a smart grid application for instance.

Recall that while IKE ensures pair-wise security associations between various peers, GDOI utilizing IKE phase 1 between each GM and KS ends up with a single and common SA amongst all GMs. Additional to pair-wise SAs with IKE phase 1, GDOI also "interprets" ISAKMP/IKE to come up with a single SA for the group security domain. Simply put, as the foundation of the secure group management solution, GDOI defines single ISAKMP Domain of Interpretation (DOI). By the same token, for cryptographically heterogeneous domains, we propose multiple DOIs to be defined and implemented with GDOI residing in the satellite domain in a similar way. Also, thanks to the GDOI IPsec, the data security is implemented in a layer in the protocol stack, which is common to all satellite, UMTS, WiMAX, etc. domains, that is desired. GDOI messages perform creation, deletion and maintenance of SAs established amongst authenticated and authorized GMs. KS rekeys the group before current keys (downloaded at the time of registration by GMs) expiration. This means that to avoid expiration of keys, the KS is also asked to provide rekeying for the group by pushing the rekey message down to GMs. This message entails the new IPsec policy and keys to be used upon expiration of the previous keys. For an up-to-date version of keying materials, the rekey message is supposed to be dispatched before the current SA expires.

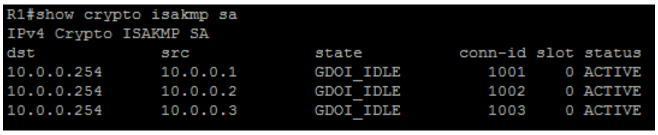
According to Figure 2, the switch within the cloud (SW1) represents the underlying infrastructure; be it satellite link/air interface or a leased wired private WAN link. This implies that regardless of what the core technology and underlying networking infrastructure/medium is (namely satellite, IP or Internet cloud, private WAN, MPLS, ATM or Frame Relay), GDOI meets the expectations (platform-independent). R1 acts as the KS as well as PDP illustrated in Figure 1 here (Cisco IOS on R1 is capable of being coded as a server). R2, R3 and finally R4 are our GMs which are required to share the same SA under a single DOI with GDOI to communicate securely. GMs can be thought of as the meter aggregation nodes in Figure 1. They will be in possession of a single unique group key for the established group (i.e. this is KEK, KEK is also called group key, and the group key encrypts TEK which in turn decrypts application data). Note that KS as well as PDP are located in the satellite domain to enable adaptive and scalable group key management for multiple DOIs.

We assigned IPs within the same subnet for all the interfaces facing SW1 from the range 10.0.0.0/24. Therefore, R1's interface is assigned with 10.0.0.254/24, R2's with 10.0.0.1/24, R3's with 10.0.0.2/24 and R4's with 10.0.0.3/24. Loopback interfaces are required to represent the subscribers into IGMP [20] for the multicast group (for a given smart grid application for instance) and thus 10.100.0.1/32, 10.100.0.2/32 and finally 10.100.0.3/32 are configured on the loopback interface number 0 on R2, R3 and R4 respectively. We then configured PIM Sparse Mode [21] for multicast routing on all the GMs. Additionally, R2 is set to play the role of the Rendezvous Point (RP) for the multicast routing protocol. Multicast channel 239.1.2.3 is also contacted by IGMP subscribers, i.e. GMs' loopbacks for instance. Lastly, OSPF is configured in the background to ensure full IP connectivity and reachability.

B. Emulation Results

We first emulate the ISAKMP session between each GM and the KS so that GM authenticates itself initially and the admission control is performed. Here, the pre-shared key (PSK) approach which is cryptographically lighter for peer authentication is preferred over Public Key Infrastructure (PKI) since resource constraints of satellite service are considered. However, a limited number of the IKE interactions at the end are merely involved for each GM-to-KS registration and thus the implementation is still scalable. IPsec SA parameters are afterwards defined which determine the traffic protection policy on the KS. This includes which traffic (via an Access Control List - ACL) needs protection and the algorithm/method that meets the given authentication/integrity/encryption requirements. Last but not least, the rekeying policy such as rekeying method (unicast or multicast), key lifetime and the retransmission rate are addressed on the KS. GMs can now (mutually) authenticate the KS and subsequently join the DOI.

By finishing the registration of GMs into the KS, on the KS, we list the GMs which have Active status for the DOI to verify the correct GDOI implementation. Remember that the ISAKMP session between the GM and KS (illustrated by GDOI_IDLE) will time out after the configured ISAKMP lifetime. This is because an ISAKMP/IKE session is only needed for the initial registration and does not need to stay up for normal secure group management operation. A rekey SA (indicated by GDOI_REKEY state) however always stays in the IKE database. The result is displayed in Figure 3.



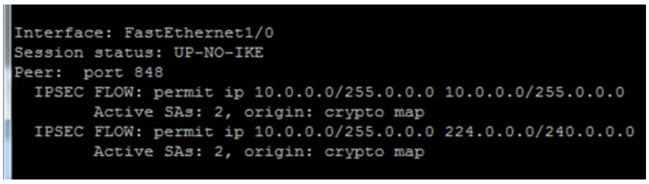
```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.254      10.0.0.1        GDOI_IDLE         1001    0 ACTIVE
10.0.0.254      10.0.0.2        GDOI_IDLE         1002    0 ACTIVE
10.0.0.254      10.0.0.3        GDOI_IDLE         1003    0 ACTIVE
```

Fig. 3. Confirming the current IKE SA on the KS after registration; each SA, assigned with the distinct connection ID in Active Status for (KS, GM) pair, is currently in GDOI_IDLE state.

Upon accomplishment of the registration phase, we next verify GDOI IPsec SA (not IKE SA discussed above) on R4 as the GM and its session status to confirm proper group IPsec SA establishment belonging to our DOI. Remember that this is where the network has already converged after a while. Convergence means that there is no added multicast traffic except the scenarios' default ones including PIM, IGMP, etc. TEK as part of the IPsec SA then encrypts the data for the DOI while KEK facilitates the rekey before IPsec expires or upon new policies being enforced.

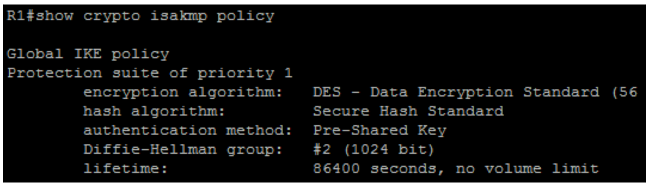
According to Figure 4, we observe that while we have not pushed down any ACL for specifying the interesting traffic (which needs to be secured) or determined any protection policy on the R4 as a GM, upon registration into the KS, GDOI IPsec SA for the DOI including policy as well as ACL is successfully downloaded from the KS and installed on the GM. Consequently, R4 then encrypts any traffic destined for other GMs of the DOI group or multicast address defined earlier based on the ACL associated with the GDOI SA.

We then verify the ISAKMP policy defined on the KS (in addition to the default policy). With the non-default IKE policy with priority 1, DES is the encryption algorithm, SHA-1 is the hash algorithm utilized, PSK is exploited as the means of authentication method, Diffie-Hellman (DH) group identifier is set to 2 within the policy and finally lifetime of the IKE SA is set to 86400 seconds (can be tuned based on the traffic volume as well). This is revealed in Figure 5.



```
Interface: FastEthernet1/0
Session status: UP-NO-IKE
Peer:  port 848
  IPSEC FLOW: permit ip 10.0.0.0/255.0.0.0 10.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
  IPSEC FLOW: permit ip 10.0.0.0/255.0.0.0 224.0.0.0/240.0.0.0
        Active SAs: 2, origin: crypto map
```

Fig. 4. Verifying GDOI IPsec SA corresponding to the DOI group on R4, as the GM, downloaded from the KS; GDOI IPsec SA's associated ACL dictates encrypting both GM-to-GM as well as GM-to-Multicast traffic within the group.



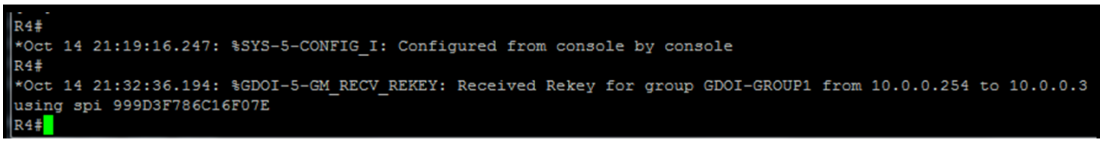
```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   DES - Data Encryption Standard (56
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Fig. 5. Group SA Policy is verified on the KS; that is algorithms, methods and thresholds which include encryption, hash, authentication, DH group identifier and lifetime within the IKE policy.

As soon as the lifetime of the first SA expires (the first 1800 seconds elapse), on the KS's console, we are informed that the first rekey is sent with sequence number 1. This informational syslog will also indicate the value of the IPsec Security Parameter Index (SPI). The substantial observation is that this SPI is shared amongst all the GMs for this DOI. We can now expect the proper receipt of the first rekey messages on the GMs dispatched from 10.0.0.254. This can be verified immediately on the GMs' consoles as Figure 6 for R4 highlights.

VI. Performance Evaluation

Strong security incurs costs and as a result most of the security proposals significantly increase the performance overheads. Here, we evaluate the added overhead of the emulated secure group management implementation for our satellite scenario with three GMs and one KS aiming at quantifying the burden imposed by the protocol in terms of the protocol message signaling. We examine the relevant Wireshark flow graph to highlight the secure group management protocol's message signaling overhead in reality for the scenario. The screenshot depicted at the bottom of Figure 7 is where R4 starts registering into the KS with the aid of GDOI. Accordingly, six plus four bidirectional messages are detected initially, exchanged for both phases (GDOI IPsec Phase 1 and Phase 2) in total. Afterwards, any communications from R4 destined for either any multicast addresses (presented here by PIM protocol messages, IGMP protocol messages) or other GMs (GM-to-



```
R4#
*Oct 14 21:19:16.247: %SYS-5-CONFIG_I: Configured from console by console
R4#
*Oct 14 21:32:36.194: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GDOI-GROUP1 from 10.0.0.254 to 10.0.0.3
using spi 999D3F786C16F07E
R4#
```

Fig. 6. R4’s console upon the receipt of the first rekey for the group from the KS. The SPI shared for the group is 999D3F786C16F07E which is the same for the entire DOI.

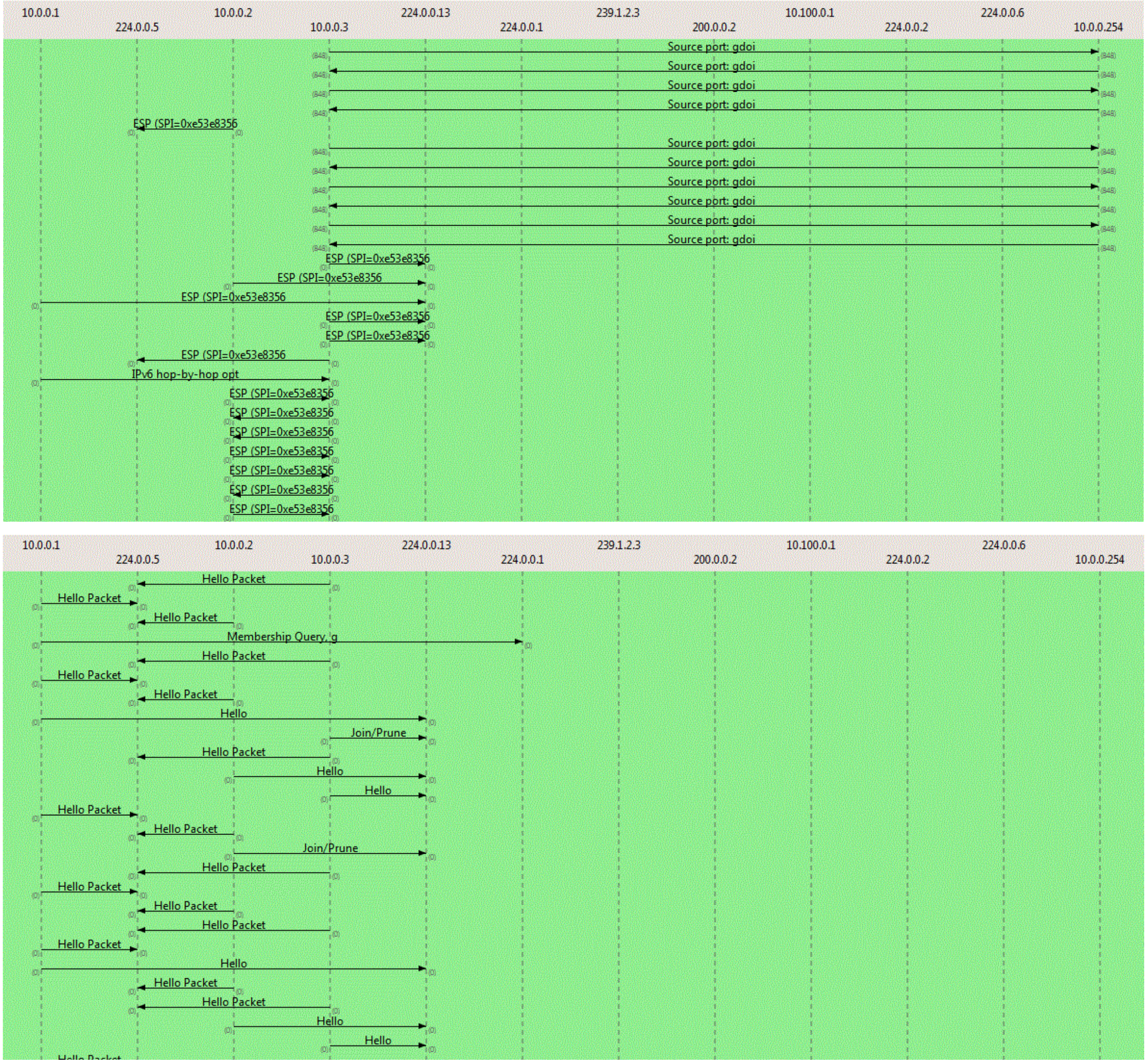


Fig. 7. Top: message signalling overhead for the secure group management protocol whereby R4 registers with the KS are detected by Wireshark, 4+6 messages are exchanged over UDP for effecting GDOI's IPsec phase 1 & 2 in total. Bottom: whereas before GDOI is in place all R4-to-GMs or R4-to-multicast-groups communications were in plaintext/unencrypted/analyzable by eavesdropper and thus unsecured, with GDOI they are all ESP protected.

GM) are encrypted and thus ESP protected. Additionally, our results here confirm that the entire domain/group communications (be it GM-to-GM or GM-to-Multicast Addresses) are secured/encrypted with the same SPI (SPI is sent in plaintextand thus is detectable) which is shared across the whole DOI. Figure 7 on the top, however, stresses the fact that the entire communications sourced from/destined for R4 before the GM joins the DOI were in plaintext (eavesdropping was feasible as the vulnerability pinpointed in section III), unencrypted (and therefore analyzable with Wireshark) and thus unsecured.

VII. Conclusion

Security has been one of the obstacles for both satellite services as well as smart grid group applications such as SCADA, Teleprotection or Security Surveillance, especially with logical/geographical/cryptographic domains spanning heterogeneous networks and regions. Innovative security

978-1-4799-5893-1/14/$31.00 ©2014 IEEE

architecture was proposed and deployed in this paper to clarify the security challenges, with a particular focus on the secure multicast key management and policy provisioning. A fixed network scenario was presented for the smart grid group applications over satellites. For such centralized architecture, the Group Domain of Interpretation (GDOI) was deployed and critically evaluated in terms of the added signaling overhead in a basic scenario. The experimental results confirmed that the eavesdropping risks were eliminated thanks to the cryptographic group management protocol, while the analyzed protocol message signaling overhead in practice does not seem to act as much of a deterrent for the solution adoption.

Future work aims in addition at estimating the overhead added by data security payload with ESP as the heart of GDOI before and after cryptographic group management protocol implementation; this reveals the added workload on the satellite system for the basic scenario which demonstrates how the proposed solution scales with the increase in the number of groups/GMs.

References

[1] B. Adams, Interdomain multicast solutions guide. Indianapolis, IN: Cisco Press, 2002.

[2] S. Yingli, H. Cruickshank, M. Moseley, and J. Ashworth, "Security architecture for satellite services over cryptographically heterogeneous networks," in Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on, 2011, pp. 1093-1098.

[3] A. J. McBride and A. R. McGee, "Assessing smart Grid security," Bell Labs Technical Journal, vol. 17, pp. 87-103, 2012.

[4] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," ed: RFC 4301 (Proposed Standard), 2005.

[5] F. Alagoz, Gu, x, and G. r, "Energy Efficiency and Satellite Networking: A Holistic Overview," Proceedings of the IEEE, vol. 99, pp. 1954-1979, 2011.

[6] Z. M. Fadlullah, N. Kato, L. Rongxing, S. Xuemin, and Y. Nozaki, "Toward secure targeted broadcast in smart grid," Communications Magazine, IEEE, vol. 50, pp. 150-156, 2012.

[7] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," Communications Magazine, IEEE, vol. 51, pp. 42-49, 2013.

[8] M. Erol-Kantarci and H. T. Mouftah, "Smart grid forensic science: applications, challenges, and open issues," Communications Magazine, IEEE, vol. 51, pp. 68-74, 2013.

[9] M. Yilin, T. H. H. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig, and B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE, vol. 100, pp. 195-209, 2012.

[10] C. Caini, H. Cruickshank, S. Farrell, and M. Marchese, "Delay- and Disruption-Tolerant Networking (DTN): An Alternative Solution for Future Satellite Networking Applications," Proceedings of the IEEE, vol. 99, pp. 1980-1997, 2011.

[11] M. P. Howarth, S. Iyengar, S. Zhili, and H. Cruickshank, "Dynamics of key management in secure satellite multicast," Selected Areas in Communications, IEEE Journal on, vol. 22, pp. 308-319, 2004.

[12] Y. W. Law, Z. Gong, T. Luo, S. Marusic, and M. Palaniswami, "Comparative study of multicast authentication schemes with application to wide-area measurement system," presented at the Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, Hangzhou, China, 2013.

[13] B. Weis, S. Rowles, and T. Hardjono, "The Group Domain of Interpretation," ed: RFC 6407 (Proposed Standard), 2011.

[14] L. Yee Wei, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," Communications Magazine, IEEE, vol. 51, pp. 34-41, 2013.

[15] H. Harney, U. Meth, A. Colegrove, and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol," ed: RFC 4535 (Proposed Standard), 2006.

[16] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," ed: RFC 2408 (Proposed Standard), 1998.

[17] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," ed: RFC 5996 (Proposed Standard), 2010.

[18] (January 2014). Graphical Network Simulator. Available: http://www.gns3.net/

[19] G. Combs. Wireshark. Available: http://www.wireshark.org/

[20] B. Haberman and J. Martin, "Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction," ed: RFC 5186 (Informational), 2008.

[21] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)," ed: RFC 4601 (Proposed Standard), 2006.

978-1-4799-5893-1/14/$31.00 ©2014 IEEE