International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

A Survey Paper on Security Issues in Satellite Communication Network infrastructure

Syed Muhammad Jamil Shah, Ammar Nasir, Hafeez Ahmed

Department of Electrical Engineering,

Institute of Space Technology, Islamabad

engineerjamz@gmail.com, Contact No. 0092-312-6840511

Abstract— Satellite communication is one of the most popular next generation communication technologies for global communication networks in parallel to terrestrial communication networks. In modern age military intelligence, navigation & positioning, weather forecasting, digital video Broadcasting (DVB), and broadband internet services, are the few demanding applications of Satellite communication. Although Satellite communication is cost effective solution for such long distance communication application, However security over the link is still a major concern in satellite communication. Due to limitations such as high bit error rate, power control, large distance between end nodes, high link delays because of large round trip times, and link availability, common security techniques incorporate a lot of issues in implementation of proper secure communication over the satellite links. In this survey paper, we explore the importance of security, trivial and currently deployed security tools, and the limitations to be considered while deploying such security techniques and protocols for securing satellite communication. Finally we reported some future research space in process to further optimize the security tools and measures for the proper security frame work over the satellite communication infrastructure.

Keywords— Satellite Communication, Security, PEP, IPsec, VPNs, Encryption, SSL, AKE.

INTRODUCTION

With the advent of satellites, the communication has been revolutionized. It is no longer viewed as a simple bent pipe but as an important component of a large global communications networking system, requiring interoperability between satellite and terrestrial communication components and thus compatible protocols and standards. Satellite networks provide global reach and wide area coverage to remote, rural and inaccessible regions. A few of its common applications include weather prediction, telephony services, telemedicine, multimedia services, internet connectivity, navigation through GPS, imaging through remote sensing satellites for resource monitoring and many important military applications. It is becoming critically important that satellite networks should be able to offer convincing networking solutions in the rapidly changing field of communications dominated mobility, personalization and high capacity demands [1].

However, with the increasing utility and demand, the need for security increases in satellite communication. The users of this mode of communication along with all sorts of benefits in terms of Quality of Service (QoS) and reduced cost of services also demand confidentiality and integrity of their data. This is particularly important in the case of military applications. Eavesdropping and active intrusion are serious concerns especially for people who transfer sensitive data over satellite link and these actions are much easier in satellite networks because of the broadcast nature of satellites as compared terrestrial fixed or mobile networks.

Moreover it is reported that, satellite channels experience long delays and high bit error rates, which may cause the loss of security synchronization. This demands a careful evaluation of encryption systems to prevent Quality of Service degradation because of security processing [2].It is also seen that in satellite communication Protection of the satellites and links is not only the key concern for the researchers and industry, but also to provide a sound integrity and confidentiality of the downlink Earth Stations and Information Systems of the command and control systems.

In this survey paper, we provided an overview of the security and related issues of satellite communication for commercial and strategic defense communication. This survey paper focused the need for security, key issues in satellite communication security, the limitations in a satellite link, and currently deployed encryption techniques that may be applied to secure a satellite link.

A brief overview of current security measures like PEP, IPsec, IPsec anti-replay, VPN based security techniques, Key exchange methods, and other such advance security measures. Then we also discussed the counter effects of such security measures over the communication system and in implementation issues in satellite networks. Finally we explored the future challenges and research frontiers in secure satellite communication that can handle the base issues still need to be addressed.

TAXONOMY OF WORK

While for the time being it is considered that a lot of advancement has been made in securing the information over the communication links. As far as it is concerned towards the security measures of wired network, to some extent this idea can be suited well, but as far as it concerned with Satellite Communication link, it still have many issues to be sorted out fully. As in satellite communication link due to its long distance, delay, more accurate power control requirements, and other concerns with the space links made it difficult for the current security measures which usually designed for the wired networks, wireless LANs or for wireless sensor networks (WSNs); to be applicable for this situation, as these security measures are not specifically designed for the such long distances space communication links like satellite uplink and down links or inter satellite links. Since satellite links have a different form of interferences and some unique interference figures. The need for satellite communication over the long distances through space communication is ever increasing demand of the time; a lot of communication traffic has been shifted towards wireless-networks, especially satellite links, which provide a cost effective, less infrastructure overhead, and a more global solution for the commercial and military applications.

In this survey paper, in section II we mentioned the need for security and then provide a comprehensive list of currently cited security issues and the impact over the satellite communication network that need to be consider while looking at the secure satellite communication. In section III of this literature we surveyed the issues with satellite link security protocols as security measures in a

In section IV, a detailed survey on security concerns with satellite communication networks infrastructure is provided. Since a lot of literature published on satellite information system security concerns, while implementing Transport and Application layer security protocols like ipsec, vpn, and PEP. Then in section V, a detailed analogy of literature on DDoS attacks and Attack tracing mechanisms is reported. In section V, ASC (American Satellite Company) work regarding security issues in satellite communication ground based command and control stations is overviewed to emphasize the command stations security concerns.

Finally in section VI of the survey paper, we focused some future research concerning areas related to more secure commercial satellite Communication. In concluding part VI of our work we tried to emphasize the security concerns which are still under consideration and need to be worked out for the better security solutions in satellite communication to maximize the reliability, confidentiality, and integrity over the satellite links to meet the next generation space and terrestrial hybrid communication trends using the secure satellite links.

SECURITY ISSUES IN SATELLITE COMMUNICATION

A well designed implementation of satellite communication networks is usually the prime concern in order to allow its usage for certain sensitive scenarios like secure defense and strategic purposes, and reliable communication through the public media. However, while deploying security in satellite communication, it is common to face some issues caused either by the characteristic of the satellite link such as the long end-to-end delay and higher bit error rates requirement for high carrier to noise power ratios C/N over the uplink and downlink. Protocols typically and frequently used in satellite networks, such as Performance Enhancing Proxies (PEPs) or IP Multicast IPsec [1] [2] to improve the efficiency in time and bandwidth of data transmission over the costly and scarce frequency bands, also contribute to the above stated issues.

In this section of survey paper we have discussed firstly why we need security and then examined few important issues related to satellite communication link and payload security.

A - Why need security?

As world of internetwork expanded need for the security over communication link as well as over endpoints (source & destination) also became one of the major concerns for the service providers, operators, and researchers.

In 2003, a research team at Los Alamos National Laboratory, USA, demonstrated how spoofing attack can be implemented on GPS. A GPS satellite simulator was used to broadcast a fake signal that caused the GPS receiver to operate as though it were located at a position different from its actual location [3].

Similarly in 2007 and 2009, a research team at Stanford University decoded Galileo in-orbit validation element A (GIOVEA) and Compass-M1 civilian codes in all available frequency bands [4]. These events emphasize the need to secure communication in satellite networks along with coding techniques.

Communication security means integrity and confidentiality in delivery of information. Researchers describe security in terms key features like confidentiality, authentication, integrity, access control, and key management; so that entity remains error free and well intercepted on the target receiver [3]. While dealing with the security in satellite communication these key points always remain a major concern for the security measures. In general we can define the security particulates as following [4] [5]:

Confidentiality means that only the appropriate users have access to the information.

Authentication requires verification of a user's identity and right to access. It is achieved using a public key interchange protocol that ensures not only authentication but also the establishment of encryption keys [6].

Integrity means that the information has not been corrupted.

Access control ensures that the system cannot be compromised by unauthorized access (e.g. pirating a satellite).

Key management is the way how to manage the security keys (how dynamically generated, concealed and distributed, finally how well-kept by the actual target) users. Key Management is a key issue with respect to IPsec over multicast Satellite Communication.

Security over the satellite link is always a key feature for the military and state departments. There always arise issues in security of the link due to number of attacks from the intruders to disrupt the link as well as tarnish data integrity, and confidentiality. Here it is a matter of key concern for the Military operations success that the communication facility they are acquiring from the satellite networks must ensure a high level of confidentiality and protection; Satellite security system must deny any sort of antagonist access to the information system that always considered as a mission critical data for the national security.

On the other end, the satellites for commercial communication, which are also time to time used for military communication objectives in temporary bases, the satellites mostly part as repeaters over the sky, and unlike the military owned satellites, the commercial satellites are not necessarily supposed to carry bulk of encryption data in space trajectories for the downlink telemetry command and control systems and earth station data and information stations. As for the commercial applications, Satellite operators mostly keep less overhead over the in-orbit satellite transponder and links to ensure the maximum cost effectiveness of the satellite link for the business gains. So, for a trusted and protected communication over the leased satellite link most of the security measures are deployed at the ground stations.

Moreover, in literature we find that as satellite networks are usually wireless broadcast networks over the downlink, the issue of eavesdropping [7] is one of the prime concerns. So appropriate security measures requirement become vital there.

B - List of Security Issues in satellite communication network infrastructure

1. Scanning/attacking
2. Jamming
3. Miss positioning/Control
4. Transponder spoofing/direct commanding.
5. Security Key management issues
6. Satellite based hybrid networks security implementation issues

7. Satellite based broadband multicast networks security implementation issues
8. TCP based security implementation issues in Satellite Networks infrastructure.
9. VPN Implementation based Security issues in Satellite communication infrastructure.
10. Ground Stations, Telemetry and command systems protection issues.
11. Denial of Service attack (DoS and DDoS attacks) issues.
12. Miscellaneous command and infrastructure security issues.

ISSUES WITH SATELLITE LINK-SECURITY PROTOCOLS

To establish a secure channel between end nodes, we use a protocol called the authenticated key-exchange (AKE). In this protocol two parties communicate after they have shared a common key between them. AKE protocols are either based on symmetric or asymmetric cryptography. The symmetric approach requires a large number of pairwise keys. Basically the long-term symmetric key is generated before executing the key-exchange protocol. In case of satellite networks, generating and managing these keys are highly problematic and thus inappropriate for scalable satellites [2]. In certificate based-asymmetric approach, each node obtains a public key of the other and verifies it with a trusted third party. But unfortunately due to the long time delay in data transmission over a satellite link, certificate based AKE protocols perform inefficiently. Furthermore the method demands a node to acquire certificate of the other node from a certificate authority and then access the certificate revocation list so that the two nodes extract each other's valid public keys, imposing extra burden on the communication channel [2]. To eliminate this burden, an identity based cryptosystem was introduced in which the nodes' public keys can be arbitrary string that serves as identity string and the intervention of the third party certificate authority is avoided [25].

The early AKE schemes such as "the identity-based scheme providing zero knowledge authentication and authenticated key exchange" [26] or "the identity-based key exchange protocol," [27] never took into account the possibility of active intrusion and hence provided little security. Most of the more recent identity-based AKE protocols such as "the two-party identity-based authenticated key agreement," [28] and the "Identity-based Authenticated key agreement protocol based on weil pairing," [29] establish session key by employing pairing techniques to secure communication against attacks. These protocols involve great number of multiplications hence are computationally inefficient. In addition, in most of these schemes, a participant's identity must be mapped to a point on an elliptic curve, and this is computationally expensive [2].

A modular approach was proposed [30] which uses application of identity-based signature scheme. The Diffie-Hellman (DH) protocol is constructed using the same technique of identity-based signatures [31]. The AKE protocol built using DH platform is known as Authenticated DH (ADH) or the Canetti-Krawczyk (CK) protocol [32]. But the downside of this protocol is that it uses three round of message transmission whereas most AKE protocols only use two rounds [2].

These protocols needed to be analyzed for security, so it was for Bellare and Rogaway to present the first security model, the BR model in 1993 [33]. Since then many extensions have been done in order to increase the level of security along with computational efficiency. The most famous extended BR model is the CK model [32] which was proposed in 2001. However, all these models followed an assumption that the attacker is not allowed to obtain certain secret information about the session that is being attacked hence leaving the AKE protocols stated above still prone to leakage of short-lived secret or private key [3].

But with the researchers with their heads down, working hard, the problem at hand has been addressed. A model that is resistant to the above mentioned attack has been reported known as the extended CK (ECK) [34]. According to this model, the only attacks that are not allowed are those that would trivially break an AKE protocol. In other words an attack in which the adversary reveals the ephemeral secret and the static private key of one node in the protocol so that this node can be impersonated. Thus, the ECK model is currently regarded as the strongest security model for AKE protocols [3]. ECK security also implies key generation center (KGC) forward secrecy [35], which helps ensure the security of previously established session keys after the master key of the KGC has been compromised.

SECURITY ISSUES BASED ON SATELLITE COMMUNICATION NETWORK INFRASTRUCTURE

In addition to satellite link securing issues, there always remain a constant amount of issues in ground station based network infrastructure and communication protocols. In this section of the survey paper we visited few key communication infrastructures issues which are equivalently encountered in both wired and wireless environments, inclusive satellite communication networks.

Moreover it is successively reviewed in satellite communication related literature that due to long delays and power limitations and free space interferences, these security issues become more hazardous if proper precautions not adopted in satellite communication.

A - Security Issues with Satellite Based Hybrid Networks

There are several security challenges with hybrid communication systems which use satellite as a part for back haul or as intermediate, which are reported time to time by keeping in view the following considerations about satellite systems:

1. As we already discussed the broadcast nature of satellite channels, which actually does not limit any unauthorized user to receive the signal and eavesdrop on the unencrypted or poorly secured satellite communication link is easily possible.
2. In case of poor link security, a well-equipped combatant can easily jam or intrude the communication link by sending false commands to the satellite.
3. In bad weather conditions like rain or cloudy condition, satellite channels face burst of errors and result in loss of packets too, which in turn also cause loss of data integrity.
4. Satellite Communication experiences long propagation delays of an order of about 0.56 seconds for geostationary satellites [20] (at a distance about 35785 km or more from earth). So security systems should be such that it cause minimal delays to the communication over the link and have an efficient mechanism of recovery from such errors.
5. Loss of message integrity or modification issues are also commonly reported security threats. Which may be removed by proper integrity checksum like MAC[24] on satellite receiver but in commercial satellites such facility is limited, and can't be provided to every message.
6. Denial of Service DoS Attacks are possible over the satellite transponder due to the limitations of its power and processing capability, and it may become a single point of failure in network to cause a hazard for whole infrastructure.
7. To provide some level of security over such scenarios encryption methods deployed, but it is seen that it also create two fold issues, selection of encryption technique and then management of encryption keys [24].

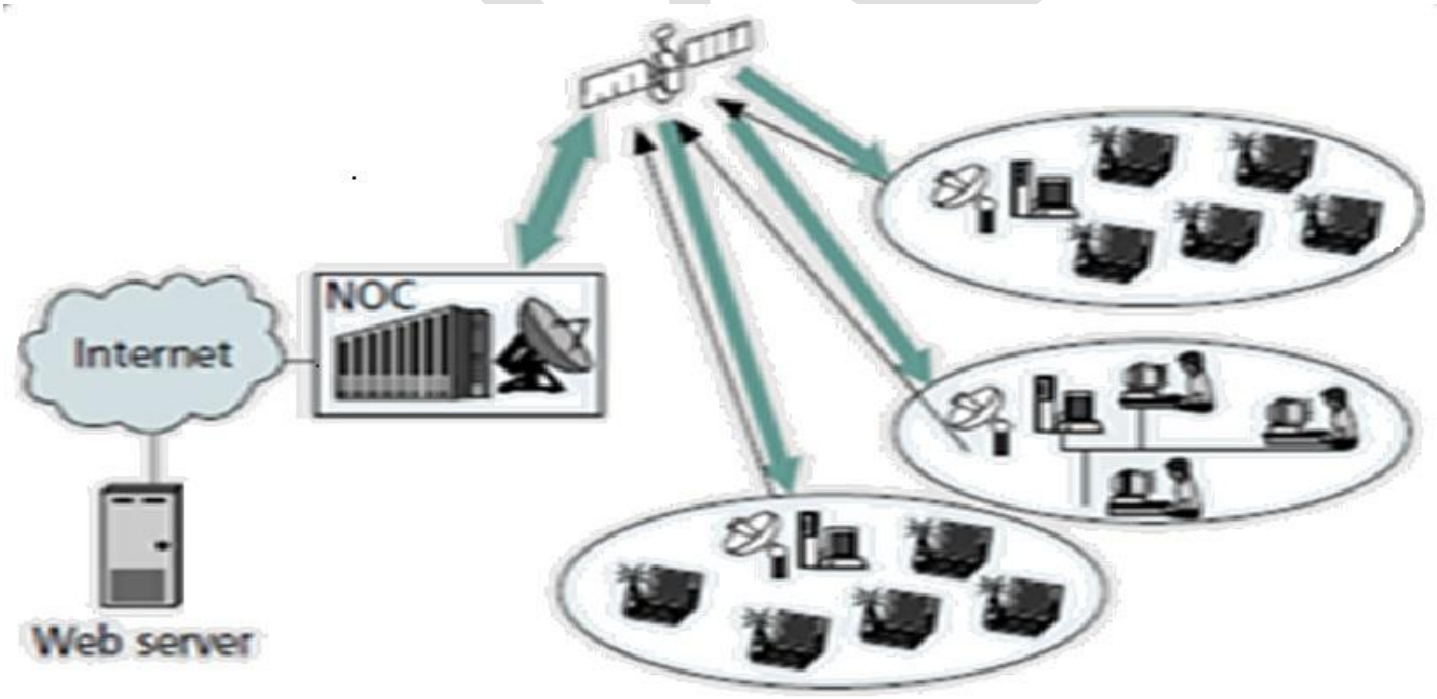

Fig. 1 hybrid satellite based communication network [14]

B – Issues with IPsec and SSL in Satellite communication

Internet Protocol Security (IPsec) must provide authentication, access control, integrity, confidentiality and key management [1]. It is reported that IPSec being considered as IETF standard End to End secure tunneling based data transfer protocol, so it is also used for satellite communication networks.

In literature about satellite communication security in unicast environment, it is also reported that Originally Terrestrial networks designed protocols, such as Internet Security Protocol (IPsec) or Secure Socket Layer (SSL) [14], when tried to implement in satellite networks, causes severe performance degradations and link overloading.

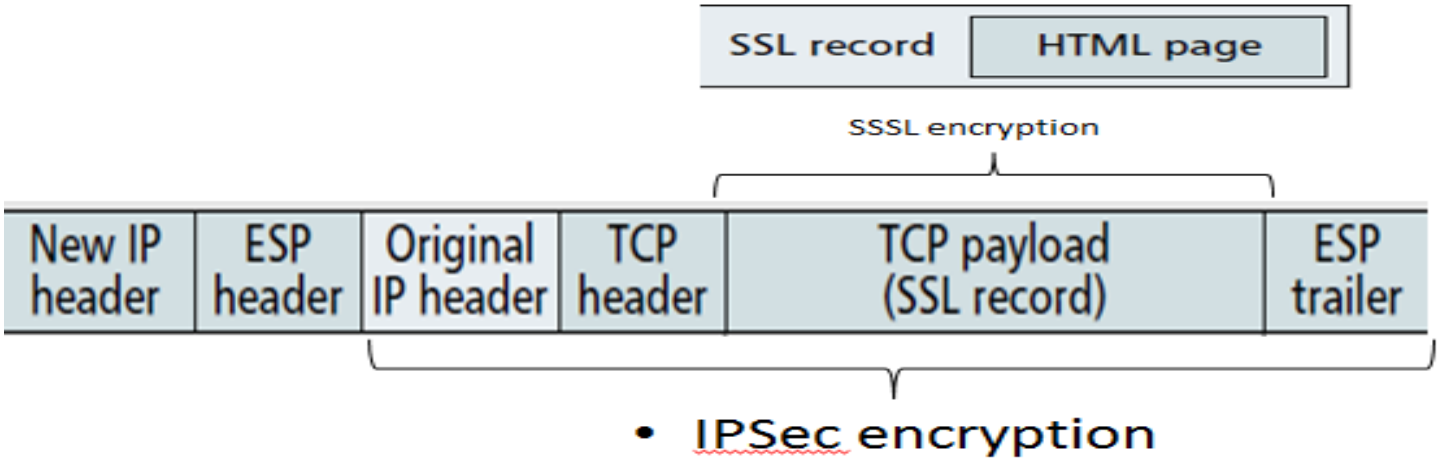

Fig.1. Traditional IPSec and SSL encryptions

Moreover it is also reported that IPSec has large bytes overhead for authentication and integrity checks services using ESP [24].Detailed study on IPSec protocol also explored that it was originated for p2p communication security, so it lacks multipoint or broadcast communication environment, as it doesn't provide dynamic key generation [24]. So IPSec have certain security implementation limitations.

It is also observed that due to the IPSec property to not allow any intermediate nodes authentication or decryption by key exchange elsewhere except end to end nodes, so PEP can't read the encrypted TCP header, so IPSec doesn't work with PEPs protocol. Similarly HTTP Proxy can't work its prefetching function, due to inability to read TCP header, which leads to a serious degradation of performance in satellite based network infrastructure.

Further during the survey, we found that to address the performance limitation issues of SSL or IPSec, researchers developed transient protocol types like HTTP over IPSec tunnel [24][49][50], Dual-mode SSL for HTTP optimization[24] DSSL.

In effort to optimize the performance and compatibility issues of IPSec and SSL, changing in the mechanism cause other adversities in performance. Like Layered IPSec cause increase in bytes overhead by almost three times more than that of original version. When we examined the SSL solution as DSSL it also provide other performance depreciation issues like complexity in design, larger overheads due to two different keys deployment. Therefore it can be concluded that IPSec and SSL improvements are considerable but still require more work to be done for lesser overheads in authentication and encryptions and simplicity in design to work with http proxy servers for better system performance in terrestrial as well as satellite communication networks.

Following table provides an overview for the Comparative study of IPSec vs. SSL security protocols.

Parameters	**SSL family protocols**		**IPSec family protocols**	
	SSL	DSSL	IPSec	Layered IPSec
Security	Unicast	Unicast	Unicast	Unicast
Implementation	End-to-End	End-to-End	End-to-End	End-to-End
Implementation Layer	(between application and transport layer)	(between app. & transport layer)	Network Layer	Network Layer
Bytes overhead	Less overhead then IPSec	Heavy bytes overhead increased	Heavy bytes (about 34 bytes)	Three times more heavier bytes overhead.

Design complexity	Less complex	More complex	Less	Medium
Group communication	No	No	No	No
Performance with PEP	Yes	yes	Severe degradaton	Yes supports PEP, Better performance
Performance with HTTP Proxy	Yes, HTTPS is main example	Yes Supports, less performance degradation	Severe degradaton	No support, so still degradation of performance

Table.1. SSL vs. IPSec comparison

C - Security Issues with Broadband Multicast Satellite Communication

In multicast satellite communication due to broadcast nature of satellite links appropriate addressing and security measures are essential to provide service to only authorized users. A highly optimized and efficient key generation and update mechanism is a key for the Multicast applications which are dynamic in nature.

Although Satellite Communication is the key technology for global communication, but Satellite systems are typically resource limited, which means links are constrained in channel capacity, Power controls, processing speeds, and switching capabilities, throughputs, link availabilities, Which in turn bounds the Link budgeting and network design of a Satellite Network.

Security issues arise with the use of protocol functionalities such as IP Multicast, mobility support functions for end systems, and Path MTU discovery used in Broadband satellite communication for the purpose of proper broadcast link management and mobility management. Similarly while using Security techniques like PEPs (Performance Enhancement Proxies) and IPsec anti-replay [1] [2] protection used for some degree of QoS insurance in satellite communication links; some decrease in performance of these protocols characteristics over the link also incorporates. Few such link characteristics are:

1. High link Latency (satellite link more specifically)
2. Large Error Rates (mostly for Wireless and Satellite links (under Rain Conditions due to effect of rain over system Noise temperature and degraded link availability)
3. Links with unequal transmission Rates, mostly high data rates at downlink, while lower on uplink (again mostly satellite links which are A-symmetric in nature) PEPs features are briefly given by IETF documents (RFC 3135), [2].

Some of the novel features about PEPs are [2] following:

1. A-symmetric/Symmetric PEPs.
2. Distributed (used in satellite links)/Integrated (in peer relationship) PEPs.
3. Layered approach PEPs (Transport/Application layer PEPs).
4. Variable Degree of Transparency (w.r.t layer in which operational)

D - TCP based Security implementation Issues in Satellite Communication Networks

Transmission Control Protocol (TCP) generally considered well for end-to end connections like wired Internet services. However, performance issues over satellite links comes due to multiple factors, among those propagation delay and channel noise effects are most compelling one. Like other wireless communication links Satellite links are also major victim of Noise, which cause drop in Eb/No, as a result of which Bit-error-rate (BER) is proportionally higher to the wired medium networks. And TCP due to its retransmission feature for reliability; is more vulnerable to high BER.TCP has no idea of whether a loss over the link caused by congestion over the link (buffer-overflow) or by corruption (noise, jamming).Moreover in Satellite Networks, TCP (which act as transport layer for Application layer protocols like telnet, http, ftp, etc.) performance declines due to the high link latency, large error rates and asymmetric links. Transport layer PEPs enhance TCP functionality which in turn eradicates issues with:

1. TCP bandwidth delay limitations over the satellite links
2. TCP slow start problem by limiting the acknowledgements and link traffic in congestion situation.

There are many Enhanced TCP approaches to increase its performance especially over the satellite links, like TCP-Scalable, TCP-BOC, TCP-High speed, or TCP-Hybla [8] [9]. But it all requires compliment with end systems, which is again a concern for the Researcher. However, a new approach of selective retransmissions using UDP as transport protocol is optimized for satellite links [13]. Application layer PEPs are used as a solution for the issue of application layer protocols enhancements, like Web Cache (HTTP proxy with caching functionality). Moreover cache enabled DNS servers can be used in the satellite communication to provide a low latency solution for the DNS queries by avoiding several round trips for this purpose in normal case. Similarly application layer proxy can provide compression, which in turn reduces the amount of data to travel through the satellite link. However, for compression and decompression a distributed PEP implementation is essential [10] [12] [13]. Since for this purpose PEPs need access of the protocol headers and payload, usually encryption or protection by network layer VPN like IPsec don't allow this [10][11][12]. So PEPs implementation causes the security issues like authentication and integrity disruption, as the PEP is not able to terminate the TCP connection [13].

INFORMATION SYSTEM BASED SECURITY ISSUES

Till now we have visited the security issues encountered with the information transmission systems. Similarly in literature issues with the protection of ground based information systems over the Satellite downlink infrastructure, such as command and control systems, information systems and the related downlink data-centers security, both in Military and in commercial satellites based networks infrastructure. As mostly it is found that military satellites specially deploy well-planned security techniques over their owned transponders and links, but in case of commercial satellites communication, where the satellite transponders mainly part as repeaters in sky, and company always seeks cost effectiveness in their business plan. So, in an effort to make the profitable business infrastructure the commercial satellites are mostly less equipped with the security tools for the downlink telemetry, command and control systems and for the related ground stations. So, for a trusted and protected communication over the leased satellite link most of the security measures are deployed at the ground stations.

The most common issue in securing the satellite information systems, Telemetry & command and control system stations include (attacks listed in table 1) [36] information systems access control attacks, injection and execution of malicious software attacks , masquerading attacks, sniffing, snooping, denial-of-service (DoS) attacks and object reusability attacks.

A. Distributed Denial of Service Attacks

Here in this survey paper we also focused DDOS[36] (Distributed Denial of Service) Attack, Another one of the most alarming one of all above mentioned security attacks in the satellite communication networks infrastructure. It is mentioned in literature in number of security attacks that a hacker or an intruder as antagonist always introduce security attacks in a flooded manner so that it can overcome the security redundancies. Similarly it is true in case of DDoS attacks.

According to the repeatedly found definition in literature of DoS (Denial of Service) [36] attacks, the DoS attack hampers the well authorized users from accessing the available resources and services. While in DDoS attack usually single to many information systems become affected due to a collaboratively and a large scale attack over the services access in the satellite based network infrastructure. But due to power and processing capability limitations over the satellite transponders, such DDoS attacks can be more violent on satellite which may become a single point of failure in communication network[14].

In Recent studies it is revealed that DoS attacks become major security concern for the host machines in the ground based Telemetry and command & control systems, and Information systems connected to the internetworks. With the advancement in hardware and software base equipment in communication industry, DDoS attacks also become more vulnerable for the communication infrastructure. Over the years DDoS attacks studies revealed that with progress the DDoS attacks tracing mechanism and their cure become more and more complicated process.

According to a deliberate study on DDoS attacks in collaborative environment[36], it is reported in a survey by Arbor Networks [37] on November 2008 that DDoS attacks scale have been ever growing since 2001. Further it is reported there that, in 2008, the largest recorded DDoS attacks against a single target reached 40 gigabits per second, more than that was reported in year 2007 of 24 Gbps. Hence, DDoS (Distributed Denial of Service) attacks are one of the alarming issues of security over the collaborative networks, and in turn a major concern for the security over the commercial satellite based communication infrastructure that often poorly equipped with

the measures to encounter the serious and advance security threats over the links. As a flooded DDoS attack can be propagated over the poorly secured satellite links by a jammer or some intruders. Similarly the probability to cause such attacks on command and control systems on ground stations is also increased over the times just due to the sophisticated attacking tools and weak security measures. Security threats due to malicious intrusion to the information and command systems, such as DDoS over the commercial satellites infrastructure; are well understood. Now these are reported as a major concern for the ground stations security in satellite communication network infrastructure.

a) Classification of DDoS Attacks

In classified study about the DDoS attacks, we found following two major categories of DDoS attacks [38], classification based on nature of Denial of Services, in which victim becomes unable to access the resources in routine.

1. The bandwidth depletion attacks: in which services and resource access are denied due to the excessive flooding of junk traffic from attackers.
2. The resource depletion attacks: in which by malfunctioning of TCP protocol to send incorrect semantic ip packets to crash the victim's system and causing critical (Processor or memory) resources depletion [36].

b) DDoS Attack Tools

DDoS attack tools are also now becoming more accessible and easier one in use to cause such hazardous attacks on the information systems. Few common DDoS attack tools [36] listed in following table:

Sr. No.	DDoS Attack Tool	DDoS Attack Class
1	Trino [39]	Bandwidth depletion
2	TFN(Tribe Flood Network) [40]	Bandwidth & Resource depletion
3	TFN2K [41]	TARGA and MIX
4	Stacheldraht [42]	Bandwidth & Resource depletion
5	Mstream [43]	Bandwidth depletion
6	Shaft [44]	Bandwidth & Resource depletion
7	Trinity [45]	Bandwidth & Resource depletion
8	Knight [46]	Bandwidth & Resource depletion

Table.2 DDoS Attack Tools Table

c) DDoS Attacks Detection

After the DDoS Attacks occurrence over the information systems and command & control stations in satellite communication network infrastructure, there arise a need for detection mechanism for such attacks. Detection of such attacks in satellite networks becomes another major challenge due to long haul communication links and limitations to delay, bandwidth, power controls and over the satellite links. Moreover with the advancement in computer systems and software products, severity of such attacks also demanded dynamic tracking mechanism for proper mitigation, particularly in satellite infrastructure.

Over the times, researcher worked for devising proper tracing mechanisms and related issues. The most reported one among all such issues, the IP-trace back mechanism definition issue.

Following table represent a comparison study of existing DDoS trace back tools and also discuss some issue, that still need to be worked on with the passage of time and advancement in communication systems and the attacking tools.

Sr. No.	Trace-back Mechanism	Mechanism Principle	Advantage	Disadvantage

1	Hash Based IP Traceback	Hashing on 28 Byte data	Low storage requirements avoids eavesdropping.	Overhead in generating 28 byte hash. increased risk of incurring false positives.
2.	Algebraic back tracing	Polynomial based trace back data generation method	Improved robustness, noise removal, multiple path construction	Changes in full path back tracing, poor scaling.
3.	Enhanced ICMP trace back	Intermediate routers based CP messages back tracing method	Less time required for full attack path tracing.	Routers require changes, Router packet Space and processing issue.
4.	Advance Hash based IP trace back	32 bits IP address hashing.	Less computational, processing , routing, and network overheads,	Require time synchronization, compromised Shared key between routers.
5.	Deterministic packet marking	Tracing information field in packet headers	Small amount of packets required for tracing.	Large size packet headers. No overload management, Intermediate processing overhead.
6.	Probabilistic packet marking	Probabilistically router marked packets	More efficient then Deterministic marking approach.	Large no. of tracing packets, Probability based approach doesn't ensure tracing, less overload mitigation, More complexity.
7.	Flexible Deterministic packet marking mechanism.	Tracing by mark recognition and address recovery mechanism.	Less amount of tracing packets, less computational overhead, high rates of tracing success.	Huge consumption of critical resource like memory for tracing.

Table.3. Current IP Tracing Mechanisms Comparison study

In latest studies over DDoS Attack tools and their tracing mechanisms, it is clearly reported that currently deployed tracing mechanisms impose following issues [36]:

1. Scalability limitations
2. Bad efficiency in case of legacy routers
3. Large computational cost
4. Large memory cost
5. Poor efficiency in term of resource consumption.

B. Miscellaneous Security issues with satellite command and control stations

In addition to the above security issues with satellite communication networks, links, and information systems; there is some documentation on the other parallel issues with the satellite networks particularly on the satellite command systems security issues and their counter measures.

American Satellite Company (ASC) [47], in collaboration with the IES (Industry Executive Subcommittee) and other forums, worked on the issues with ground station security infrastructures which were previously given no such importance to develop a sound security mechanism for the command and control stations, information systems, and TT&C stations protection. To mitigate such threats on the commercial satellite networks, ASC deployed a command link protection system with help of Commercial Satellite Survivability (CSS) Task Force, based on the DES algorithm [47]. As an overview of ASC security measures implementation, following Key security measures included:

a) Command link protection system.
b) ASC Satellite control systems.
c) ASC Satellite commands standardization.
d) ASC Satellite commands Authorization.

e) Ground based authentication system.
f) Robust key management mechanism.
g) a two-tier key, Master and Operation, approach to enhance cryptographic security of keys.
h) Redundant operational featured authentication system.

CONCLUSION

Satellite Communication is becoming more and more popular in modern day communication systems. From Commercial usage to the Military intelligence purposes, satellite based hybrid communication network architecture is becoming the ultimate future for communication engineering. But with the advancements in electronics and communication technologies the limitations of this system like long delays, link and system sensitivity towards the atmospheric effects, and larger links; are becoming more vulnerable for the hacking and rogue communication over the legitimate links. Hence Over the times number of security issues in satellite communication networks infrastructure arise, so these issues need more detail studies in the particular area, as do this survey paper focused with a brief literature review and pinpoint study over the few vital security loop holes in satellite communication systems.

Future work & Recommendations

"As the cyber security landscape continues to change with each new wave of attacks, DoS and DDoS attacks are changing as well and will continue to target organizations with more gusto than even before," said Avi Chesla, chief technology officer, Radware.int. In Radware's 2011 Global Application and Network Security Report reported that in last two years major security attacks over the Network infrastructure (both wired and wireless including satellite communication) were not only volume based but also the most threatening ones included light volume, slow security attacks. It recommends: to scale the security attacks over the information systems and network infrastructure of satellite command and control stations like, DoS and DDoS attacks, a precise measure of attack size, attack type, and frequency of attack must be collected to device a correct measure for the security attack.

So more research work on such topics is required to optimize the Security solutions for the rapidly mounting Denial of service attacks, especially for the delay, power, and resource limited communication networks.

Issues with IPSec and SSL security protocols which considered as IETF adopted protocols, need to be optimized further to remove the design complexity issues in DSSL, ML-IPSec increased bytes overhead issue, to make them ideal security protocols for the upcoming challenges both in satellite and terrestrial network infrastructures.

Similarly a robust key exchange mechanism over the satellite link is still an open frontier for the developers and security experts. Since recently a study reveals the vulnerability of RSA codes security. RSA key extraction performed using acoustic cryptanalysis [48], while putting one of the advance key encryption mechanisms under threat of being breached. So new security issues, in addition to previous ones, born with such sophisticated attacks over the encryption mechanism.

REFERENCES:

[1]Mihael Mohorcic, Ales Svigelj, Gorazd Kandus and Markus Werner, "Adaptive Routing for Packet Oriented Intersatellite Link Networks: Performance in Various Traffic Scenarios", In proceedings of IEEE Transactions on Wireless Communications, No. 4, Volume 1, Pg. 808 – 818, October 2002.

[2]Zhong Yantao and Ma Jianfeng, "A Highly Secure Identity-Based Authenticated Key-Exchange Protocol for Satellite Communication," Journal Of Communications And Networks, Vol. 12, No. 6, December 2010.

[3] ETS TR 102 676 V1.1.1: "Satellite Earth Stations and Systems (SES);Broadband SAtellite Multimedia (BSM); Performance Enhancing Proxies (PEPs)", November 2009

[4]Carlo Caini, Rosario Firrincieli, Daniele Lacamera: "PEPsal: a Performance Enhancing Proxy for TCP satellite connections", Paper, July 2006

[5]Cruickshank, H, Iyengar, S, Howarth, MP and Sun. Z, "Securing satellite communications," IEE Military Satellite Communications Seminar, IEE Savoy Place, London, October 2002

[6]J. Warner and R. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," J. Security Admin, Pg. 19–28, 2002.

[7] A. Noubir and L. von Allman, "Security Issues in Internet Protocols over Satellite," Proc. IEEE VTC '99 Fall, Amsterdam, The Netherlands, Sept. 19–22, 1999.

[8] Y. Challal, H. Bettahar, A. Bouabdallah, "A Taxanomy of Multicast Data Origin Authentication: Issues and Solutions", IEEE Communications Surveys and Tutorials, Vol. 6, No.3, pp. 34-57, Oct. 2004.

[9] A. Perrig, D. Song, J.D. Tygar, "ELK , a New Protocol for Efficient Large-Group Key Distribution", Proc. IEEE Symp. on Security and Privacy, pp. 247-262, May 2001.

[10] M. Arslan and F. Alagoz, "Security issues and performance study of key management techniques over satellite links," in 11th Intenational Workshop on Computer-Aided Modeling, Analysis and Design of Communication Links and Networks, 2006

[11] Solutions for securing broadband satellite communication Wolfgang Fritsche Internet Competence Centre IABG Ottobrunn, Germany Fritsche@iabg.de

[12] C. Caini and R. Firrincieli, "A New Transport Protocol Proposal for Internet via Satellite: the TCP Hybla", in Proc. ESA ASMS 2003, Frascati, Italy, Jul. 2003, .vol. SP-54.

[13] Carlo Cainin,y and Rosario Firrincieli: "TCP Hybla: a TCP enhancement for heterogeneous networks", paper, Int. J. Satell. Commun. Network. 2004; 22:547–566 (DOI: 10.1002/sat.799)

[14] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", IETF RFC 5246, August 2008

[15] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", ietf RFC 4301, December 2005

[16]R. Fox, "TCP Big Window and Nak Options", IETF RFC 1106, June 1989

[17] M. Mathis, J. Mahdavi, S. Floyd, A. Romanow, "TCP Selective Acknowledgment Options", IETF RFC 2018, October 1996

[18] S. Kent, "IP Encapsulating Security Payload (ESP)", IETF RFC 4303, December 2005

[19] S. Kent, "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", IETF RFC 4304, December 2005

[20] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998

[21] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services", IETF RFC 2475, December 1998

[22] V. Jacobson, K. Nichols, and K. Poduri, "An Expedited Forwarding PHB",IETF RFC 2598, June 1999

[23] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, "Assured Forwarding PHB Group", IETF RFC 2597, June 1999

[24] Roy-Chowdhury A., Baras J. S., Hadjitheodosiou M., Papademetriou S., "Security Issues In Hybrid Networks With a Satellite Component", IEEE Wireless Communications, December 2005

[25]A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. Advances in Cryptology-Crypto, Berlin: Springer-Verlag, Pg. 47–53, 1984.

[26]M. Girault and J. C. Pailles, "An identity-based scheme providing zero knowledge authentication and authenticated key exchange," in Proc. European Symposium Research Computer Security, Pg. 173–184 Oct. 1990.

[27] C. Gunther, "An identity-based key exchange protocol," in Proc. EUROCRYPT, Pg. 29–37, 1989.

[28] N. McCullagh and P. S. L. M. Barreto, "A new two-party identity-based authenticated key agreement," in Proc. CT-RSA, Pg. 262–274, 2005.

[29] N. P. Smart, "Identity-based Authenticated key agreement protocol based on weil pairing," IET. Electron. Lett. vol. 38, no. 13, Pg. 630–632, 2002

[30]M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols", in Proc. ACM Symposium. on Theory Comput, 1998, pp. 419–428.

[31]W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transaction Information Theory, vol.22, no. 6, Pg. 644–654, 1976.

[32]R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," Lecture Notes Comput. Sci., Springer-Verlag, vol. 2045, pp. 453–474, 2001.

[33]M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. CRYPTO, 1993, pp. 232-249.

[34]B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," Lecture Notes Computer Science, vol. 4784, Heidelberg: Springer, Pg. 1–16, 2007.

[35]L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings," in Proc. IEEE Comput. Security Found. Workshop, 2003, pp. 219–233.

[36] Arun Raj Kumar, P. and S. Selvakumar,"Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment- A Survey on DDoS Attack Tools and Traceback Mechanisms," 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009

[37]Arbor Networks, "Worldwide Infrastructure Security Report", Volume IV, October 2008.

[38]Stephen M. Specht and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures", Proceedings of 7th International Conference on parallel and Distributed computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp.543-550, September 2004.

[39] P.J. Criscuolo, Distributed Denial of Service TrinOO, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory (CIAC), UCRL-ID-136939, Rev. 1,Lawrence Livermore National Laboratory, February 14, 2000.

[40] D. Dittrich, The Tribe Flood Network Distributed Denial of Service attack tool, University of Washington, October 21, 1999.

[41] J. Barlow, W. Thrower, TFN2K an analysis, 2000, Available from http://security.royans.net/info/posts/bugtraqddos2.shtml>.

[42] D. Dittrich, The _Stacheldraht_ Distributed Denial of Service attack tool, University of Washington, December 1999.

[43] D. Dittrich, G. Weaver, S. Dietrich, N. Long, The _mstream Distributed Denial of Service attack tool, May 2000.

[44] S. Dietrich, N. Long, D. Dittrich, Analyzing Distributed Denial of Service tools: the Shaft Case, in: Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, LA, USA, December 3-8, 2000, pp. 329-339.

[45] B. Hancock, Trinity v3, a DDoS tool, hits the streets, Computers Security 19 (7) (2000) 574.

[46] CERT Coordination Center, Carnegie Mellon Software Engineering Institute, CERT Advisory CA-2001- 20 Continuing threats to home users, 23, 2001

[47] Mr. Otto W. Hoernig, Jr. and Dr. Des R. Sood, "command system protection for commercial communication satellites" American Satellite Company1801 Research Boulevard, Rockville, Maryland 20850-3186

[48] Daniel Genkin, Technion and Tel Aviv University, Adi Shamir, Weizmann Institute of Science, Eran Tromer, Tel Aviv University, "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis" December 18, 2013

[49] Y. Zhang, "A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks," IEEE JSAC, vol. 22, no. 4, 2004, pp. 767–76.

[50] M. Karir and J. Baras, "LES: Layered Encryption Security," Proc. ICN'04, Guadeloupe (French Caribbean), Mar. 2004