SECURE AND RELIABLE DEEP SPACE NETWORKS

By

VINAY KUMAR ABBURI

Bachelor of Engineering in Computer Science

Sri Nandhanam College of Engineering and Technology

Anna University

Chennai, Tamilnadu

2005

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
July, 2007

SECURE AND RELIABLE DEEP SPACE NETWORKS

Thesis Approved:

Dr. Johnson Thomas

Thesis Adviser

Dr. Venkatesh Sarangan

Dr. Nohpill Park

Dr. A. Gordon Emslie

Dean of the Graduate College

TABLE OF CONTENTS

Chapter Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION TO SATELLITE SYSTEMS:

A satellite is an object that orbits around another object. For example, the Moon is a satellite of the Earth, and the Earth is a satellite of the Sun. Rocket or cargo bay of the space shuttle is used to carry the satellite into orbit. Satellite technology has emerged tremendously since Arthur C. Clarke first invented it. Many emerging applications will incorporate multiple spacecraft that form communications networks necessary to achieve coverage, latency and throughput requirements.

Satellite systems have the advantage of global coverage and inherent broadcast capability and offer a solution for providing broadband access to end users. Today, satellite technology is all around to bring us live coverage of events from around the world. Satellite networks play an important role in achieving global coverage by providing commercial, civil and military services. Many applications use satellite networks for data delivery. Worldwide communications using internet, telephone, television and radio ride on the presence of backbone satellites. Present day satellite networks enable people to transmit data from/to any part of the globe instantaneously. Compared to geostationary (GEO) satellites, low earth orbit and medium earth orbit satellite networks have shorter round trip delays and lower transmission power requirements. They can also be used to carry signaling and network management traffic as well as data packets.

The two most important elements of the satellite networks are the satellites and the Earth stations. Generally, data packets will be transmitted form Earth stations to satellites and vice versa.

1. *Satellites* - Satellites carry equipment like antennas, cameras, radar and transponders. Communications satellites equipped with antennas and transponders receive the original signal from the transmitting Earth station and re-transmit this signal to the receive stations on Earth. The omni directional antennas that were used in communication satellites were replaced by unidirectional, pointed antennas. Researches concluded unidirectional antennas pointing quite precisely towards the destination outperform omni directional antennas. These unidirectional antennas are steerable. A weather satellite has cameras included in its payload. Payload for satellites depends on the operation they perform. Inter-satellite links enable inter-satellite communication, while satellite-earth links are used for message exchange with Earth stations. Satellites have processing capabilities and buffers to store information for transmission. Satellites also have rechargeable batteries to supply power when it travels beyond the Sun's scope.
2. *Earth Station* – An Earth Station is located on the Earth's surface and is not mobile. Earth stations transmit or receive data using a relay backbone of satellite networks. Earth stations like satellites have antennas, usually dish, and equipped

with transmitters, decoders and receivers. In general, earth stations have high power antennas which enable large coverage distance. The type and size of the antennas used varies with the type of services provided. Earth stations are sink nodes or destinations, for a sensor satellite network. Application devices of the Earth stations transform radio signals received into information and transfers to a computer or to a destined device, like a TV if it is a broadcast program.

A satellite network, composed of mobile satellites, fixed ground stations and communication links, have characteristics such as long propagation delays, limited energy and time varying relatively high channel error rates.

a) *Mobility* - Satellites are mobile and their mobility can be pre-computed using Keplerian laws, as they rotate in their orbits. Geostationary satellites move relative to earth and are always stationary above a point on the earth. Satellite mobility balances the resource utilization among the satellites, avoiding any holes in the network.

b) *Long Propagation Delay* - Satellites communicate using inter-satellite links and use satellite-ground links to communicate with earth stations. Satellites are usually far from one another and from the ground resulting in long propagation delays. Propagation delay for deep-space communication links is variable and extremely long.

c) *Energy Constraints* - Solar energy being the only external source of energy, a satellite is equipped with solar panels to generate power.

Satellites also carry rechargeable batteries that can be used for power at times when it is out of the Sun’s view. High cost and the risk of radioactivity release in case of accidents, prevent the extensive usage of communication satellites.

d) *High Bit Error Rates* - Weather conditions largely impacts the channel conditions resulting in high bit error rates

Satellite networks are advantageous over terrestrial networks, as they are less affected by congestion; their architecture is scalable and also cover geographical locations which are inaccessible to a terrestrial network. Satellite TV can serve any individual, irrespective of how far is he from the nearest cable TV junction with digital quality television programming.

1.2 PROBLEMS IN EXISTING MODELS:

Little work has been reported on developing a secure mode of communications in a deep space satellite network. The main thrust of space communications to-date has been to provide reliable communications between ground mission control and a single spacecraft. It has become easier to compromise the protected space network by compromising the relatively insecure ground network. Threats include unauthorized access which can impact operations and lead to the abortion of a mission. Other threats include interception of data, replay attacks, jamming and software threats. For example, commands to the craft from mission control can be intercepted and be modified before being retransmitted to the craft.

The security working group of Consultative Committee for Space Data Systems (CCSDS) has published a number of green books as recommendations for security protocols at the different communication layers [8, 9]. In addition CCSDS has proposed security architectures for space communications as well as identified potential threats [8,9]. However, currently there is no infrastructure that can provide secure and reliable communication without adding much to the overheads. Further, the existing protocols also may not incorporate the constraints necessitated by the limited energy-supplies and intermittent connectivity between the orbiters. This further diminishes the applicability of the existing protocols for the given problem scenario. While some protocols have been developed for space-based networks [1], such protocols do not incorporate feedback from the physical layer and hence may result in sub-optimal performance.

Existing terrestrial key management structures are not suited for space due to the high latency and error rates. Networking protocols developed so far for mobile ad hoc networks may not be suitable for inter-space networks [1]. These protocols have been developed primarily for scenarios involving links without long propagation delays and for networks where node mobility cannot be pre-determined. While the former prevents the applicability of any such protocol for inter-space networks, the latter does not allow a protocol to take advantage of the predictable mobility patterns found in inter-space networks.

1.3 Proposed Work:

Our main objective is to develop an algorithm that can increase the reliability and security in the path while minimizing overheads such as complex computations, increased end to end delay, etc. We realize this by assigning costs to every node and link in the path and then optimally selecting a path with the lowest cost.

In the proposed algorithm, every satellite in the network is termed a node and the node at the destination/receiving end (satellite or space shuttle) is termed as the root node. The root node near earth is one hop from the ground station. Adjacent satellites can communicate with each other and share keys to enable secure communication without much overhead. During the initialization step, the algorithm generates a key graph from the physical graph with links between all possible nodes that can share a key. Here, the additional constraint on the network that differs from a traditional deep space network is that the nodes can communicate with another node within its communication range R if and only if they can share a key. Unlike mobile networks, once the connection is established, they tend to exist unless the satellites move away from each other which will be for a definite period of time. The movement of satellites is pre-determined and hence the proposed algorithm supports the system.

All the nodes are assumed to have some form of unique ID's from existing systems like CCSDS and this is used as reference for location based authentication. When they are deployed, this information can be used to localize them. Unlike the SGRP (LEO/ MEO) protocol [13], the LEO satellites not only measure the delay reports between them, but also focus on minimum energy consumption [5] and transmit this information to the node at the higher level, which transmits this to the ground station for computing the routing table information.

The input to the algorithm is a graph with random links between nodes in the graph. Hence, the goal is to develop a key graph that is built on physical graph such that the neighboring nodes can share a key. The proposed algorithm has two phases:

1. **Initialization**: In this step, the algorithm determines the potential secure links between all neighboring nodes in the graph.

2. **Determine a Secure and reliable path**: After the establishment of secure links, we would assign costs to each node and link in the graph and then use dijkstra's shortest path algorithm to find the minimum cost path.

The proposed work provides a reliable channel for communication, the use of UDP will be encouraged rather than TCP. Moreover, we can vary the packet size to ensure maximum efficiency. This may be built on open technology such as SCPS [5] for easy upgrade of software in case there is a need to solve issues that might arise in future. Furthermore, DTLS can be considered to improve efficiency [4]

The next chapter focuses on previous work in the area. The chapter following gives detailed description of the proposed algorithm with heuristics and shows how the proposed algorithm provides more reliability without affecting the end-to-end delay. The next chapter provides the results of simulation where we compare the results of our algorithm to a system where the path is determined without any such security constraints. The conclusions form the final chapter.

CHAPTER II

REVIEW OF LITERATURE

In this section we review previous work in the field. We first review the popular communication protocols – TCP and UDP. This discussion is followed by a security routing protocol in sensor networks namely Location based authentication which provides perfect network resilience

In 1945, Arthur C. Clarke first predicted that satellites in orbit approximately 36,000 kilometers above the equator, with a period of 24 hours, could maintain a fixed location as seen from the ground. In this geostationary orbit (GSO), a satellite could receive signals from the ground and transmit them over roughly a third of the Earth's surface. For more that three decades now, GSO satellites have been virtually the exclusive means of providing space-based communications (e.g., TV broadcast, long distance telephony, etc). The communications revolution is rapidly changing space – based communication services, systems and networks.

Satellite networking, using inter-satellite links, is essential to have continuous access to any part of the globe achieving global coverage and to carryout real time data transmission. A communication satellite is one used to receive and transmit data from and to any part of the globe, while sensor satellites like weather satellites are used to monitor and forecast weather conditions. Satellite sensor networks have sensors to sense the environment of our interest and transmit it to the ground stations. In general, space networks can be classified based on the operations they perform and here are the satellite network types. [12]

1. *Satellite based communication networks*

Satellites that are used in communication networks are typically geostationary satellites, so that the broadcasting station will never lose contact with the receiver. Almost all of the communication sources television, radio, telephone and newspapers uses communication satellite network with ground stations for data transmission. A communication satellite receives a signal from uplink and amplifies before sending the signal on its downlink. Data transmission in communication networks is fast and reliable, achieving live coverage to/from any part of the globe. Communication satellites carry large volumes of data compared with terrestrial networks. Satcomes communication satellites are being used increasingly to handle long distance telephone calls, television programs, and other transmission around the world.

2. *Space based Sensor Networks*

Satellites in the sensor network usually have one or more sensors onboard for sensing areas of interest. Remote sensing satellites of sensor networks study the surface of the Earth. Remote sensing satellites are spatially distributed for simultaneous sensing of multiple locations of earth. Space based sensor networks provides real-time observations by rapid dissemination of satellite sensed data like weather information, elevation measurement, air quality. The data provided by sensor web to the scientific models monitors and forecasts the implications. Some of the satellite sensor networks applications include environment monitoring, air traffic control, military sensing and video surveillance. Satellites forming sensor networks gathers data from ocean, desert, and polar areas of the Earth where conventional weather reports are unavailable or limited.

2.1 TCP: The Transmission Control Protocol (TCP) is a virtual circuit protocol that is one of the core protocols of the Internet protocol suite, often simply referred to as TCP/IP. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange streams of data using Stream Sockets. The protocol guarantees reliable and in-order delivery of data from sender to receiver. TCP also distinguishes data for multiple connections by concurrent applications (e.g., Web server and e-mail server) running on the same host. TCP does not perform well on satellite channels due to high delay bandwidth, high bit error rate and burst errors and thus increases work load on Transport and data link layer for retransmission.

2.2 UDP: The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as data grams (using Datagram Socket) to one another. UDP is sometimes called the Universal Datagram Protocol. UDP does not provide the reliability and ordering while TCP does. Data grams may arrive out of order, appear duplicated, or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for many lightweight or time-sensitive purposes. Also, its stateless nature is useful for servers that answer small queries from huge numbers of clients. Compared to TCP, UDP is required for broadcast (send to all on local network) and multicast (send to all subscribers).

2.3 SCPS (SPACE COMMUNICATIONS PROTOCOL STANDARDS): SCPS is a protocol suite designed allows communication over challenging environments. Originally developed jointly by NASA and DoD's USSPACECOM to meet their various needs and requirements. These protocols have been found to be applicable in meeting the needs of the satellite and wireless communities. [5]

SCPS, a completely open and proven technology, has met the needs of commercial, educational, and military environments. It was designed to meet the following goals:

1. Best possible use of limited bandwidth
2. High link utilization
3. Conservation of power
4. Prioritization of traffic
5. Tolerant of intermittent connectivity

6. High forward/return link asymmetry

2.4 LOCATION BASED AUTHENTICATION:

We use location based authentication in our approach as each satellite resents a potential point of compromise. On compromising certain nodes and acquiring keying material, adversaries can launch various insider attacks such as spoofing, altering or replaying routing information to interrupt network routing, launching Sybil attack where a single node presents multiple identities to other nodes, or launching identity replication attack, etc. This situation demands compromise tolerant security design. In other words, the network should remain highly secure even when a number of nodes are compromised. Moreover, this scheme enables deterministic, secure and efficient establishment of a shared key between any two network nodes be they immediate neighbors or multiple hops away.

Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. [7] To mitigate the impact of compromised nodes, we use location based compromise tolerant security mechanisms. This is based on a new cryptographic concept called pairing and by binding private keys of individual nodes to both their vicinity.

2.4.1 PRE-DEPLOYMENT PHASE:

Assumption: All nodes have the same transmission range R and communicate via bi directional wireless links. Nodes perform a collaborative monitoring of the designated sensor field and report the sensed events to the distant sink, which is the data collection center with sufficiently powerful processing capabilities and resources.

Let p, q be two large primes and E / F_p indicate an elliptic curve $y^2=x^3+ax+b$ over the final field F_p. We denote by G_1 a q-order sub group of additive group of points by E / F_p and by G_2 a q-order subgroup of the multiplicative group of finite field $F^{*}{}_{p}{}^{2}$

Tasks before network deployment:

a) Generate the pairing parameters, (p, q, E/F_{p}, G_1, G_2, ệ) and select an arbitrary generator W of G_1.

b) Choose two cryptographic hash functions: H, mapping strings to nonzero elements in G_1, and h, mapping arbitrary inputs to fixed-length outputs, e.g., SHA-1 [7].

c) Pick a random k € Z_{q} as the network master secret and set W_{pub} = kW.

d) Calculate for each node A an ID-based key (IBK for short), IK_A = k $H(ID_A)$ € G_1

Each node is preloaded with the public system parameters (p, q, E / F_{p}, G_1, G_2, e, H, h, W, W_{pub}) and its private IK_A. It is important to note that it is computationally infeasible to deduce from k either (W, W_{pub}) or any (ID, IBK) pair like (ID, IK_A), due to the difficulty of solving the DLP (Discrete Logarithmic Problem) in G_1. Therefore, even after compromising an arbitrary number of nodes and their IBKs (Identity based key), adversaries are still unable to calculate the IBKs of non compromised nodes

2.4.2 SENSOR DEPLOYMENT AND LOCALIZATION:

1. After the pre-deployment phase, the nodes are deployed in various ways - physical installation or random aerial scattering.

2. The nodes are localized using either of two localization techniques namely Range based localization and Range free localization.

a. **RANGE BASED LOCALIZATION**: A group of mobile robots are dispatched across the whole sensor field along pre planned routes which have powerful computation and communication capabilities than ordinary nodes. The robot is equipped with master secret key. In order to localize a node:

i. The mobile robot runs the secure range-based localization protocol mentioned in references to measure their respective distance to node A and the co-determine the location of A.

ii. Then it computes hash function based on its location, master secret key and its id and sends information to A. Here, encrypting message with master key refers to message integrity code (MIC) of message.

iii. Upon receipt of message, node A first uses it pre-loaded keying material to decrypt its location id and then re generates MIC. If both match, then it saves the location id for subsequent use. During subsequent network operations, node addition may be necessary to maintain good network connectivity which will be done in similar fashion.

b. **<u>Range Free localization:</u>** In this kind of localization technique, there are some special nodes called anchors knowing their own locations. All other non-anchor nodes derive their locations based on information from anchors and neighboring nodes via secure range-free localization techniques mentioned in references.

The nodes are pre-loaded with master secret key, which is used to derive their locations based on information from anchors and neighbors via secure range-free localization with assumption of secure-sensitive environment that the adversary takes time interval t which is more than the time taken to localize node and generation of location based id.

2.4.3 Location based Neighborhood Authentication:

During the post deployment phase, each node is required to discover and perform mutual authentication with neighboring nodes. Each node will think of another node as an authentic neighbor if and only if that node is within its transmission range R and also holds the corresponding LBK (Location Based Key). Suppose node A wishes to discover and authenticate neighboring nodes after obtaining its location and its LBK:

I) Node A broadcasts an authentication request including its ID ID_A and location ℓ_A and some random nonce n_A.

II) Upon receipt of such a request, node B first needs to verify the claimed distance using Euclidian’s distance $(||\ell_A - \ell_B|| <= R)$ so that adversaries cannot surreptitiously tunnel authentication messages between B and some virtual non-neighbor node. If the inequality holds then B simply discards the authentication request. Otherwise, it continues with step III.

III) It computes a shared key based as follows

$K_{B,\ A} = \underset{.}{\hat{e}}\ (LK_{\ B},\ H\ (ID_A \ \|\ \ell_{\ A}))$. It then unicasts a reply to node A including its ID and location, a random nonce n_B, and MIC computed as h $K_{B,\ A}\ (n_{\ A} \| \ n_{\ B} \ \| \ 1)$

IV) Upon receiving the reply, node A also first checks if the inequality $\|\ell_{\ A} - \ell_{\ B}\| <= R$ holds. If so, it proceeds to derive a shared key as

$K_{A,\ B} = \underset{.}{\hat{e}}\ (LK_{\ A},\ H\ (ID_B \ \|\ \ell_{\ B}))$ whereby to re-compute the MIC. If the result is equal to what B sent, node A considers B as authentic neighbor. Subsequently, A returns to node B a new MIC computed as

$h\ K_{A,\ B}\ (n_{\ A} \| \ n_{\ B} \ \| \ 2)$.

V) Upon receipt of it, B uses $K_{B,\ A}$ to regenerate the MIC and compares the result with what it just received. If they are equal, B regards node A as an authentic neighbor as well.

The above process is valid because, if and only if both A and B have a correct LBK, $K_{A,B}$ is equal to $K_{B,\ A}$ due to the following equations:

$$
\begin{aligned}
K_{A,\ B} &= \hat{e}\ (LKA,\ H\ (ID_B \ \|\ \ell_B)) \\
&= \hat{e}\ (k\ H\ (ID_A \ \|\ \ell_A),\ H\ (ID_B \ \|\ \ell_B)) \\
&= \hat{e}\ (H\ (ID_A \ \|\ \ell_A),\ k\ H\ (ID_B \ \|\ \ell_B))
\end{aligned}
$$

$$= \hat{e}\,(k\,H\,(ID_B \,\|\, \ell_B),\, H\,(ID_A \,\|\, \ell_A))$$

$$= \hat{e}\,(LKB,\, H\,(ID_A \,\|\, \ell_A))$$

$$= K_{B,\,A}$$

In case multiple nodes simultaneously respond to the same authentication request, MAC layer mechanisms like random jitter delay (every node has to wait before answering an authentication request) are used to resolve this problem.

2.5 ROUTING IN DEEP SPACE SATELLITE NETWORKS WITH LOSSY LINKS:

This paper [6] proposes routing schemes to forward packets in deep space networks with lossy links which is build on a framework proposed by Clare et. al and are sensitive to energy consumed and link error rates along a satellite link. The authors study two routing schemes CER (one that employs re-transmissions) and REL (one that does not re-transmit packets) in terms of energy consumptions, reliability and throughput. A high level description of the algorithm procedure is as given below:

1. Initialize the Process and Processed sets to Φ.
2. Find b_{max} and b_{min}
3. Add children of the branch satellite in b_{max} to the Process set.
4. Sort the nodes in the decreasing order of their energy loads.
5. While Process set is not Null,
6. For each of the satellites in the Process set,

```
        a. If there is no link from the current node to any of the other branches then proceed with next satellite in the Process set. Move the node from the Process set to the Processed set.
        b. If the node has links to other branches, choose the branch bconn with the minimum load and then check to see if Subtree Movement Criteria (SMC) holds. If SMC holds
        c. Move the node from bmax to bconn
        d. Update the child parent relations in the branches $b_{max}$ and $b_{conn}$
        e. Repeat steps 2, 3, and 4 with new $b_{max}$ and $b_{min}$
        f. If SMC does not hold, move the current node from the Process set to the Processed set
    7. End of for loop
    8. For each of the nodes in the Processed set
        a. add the immediate children nodes to the Process set
    9. End of for loop
    10. Set the Processed set to $\Phi$.
    11. End while loop
```

The authors conclude after a series of simulations that in the presence of lossy links, the proposed bit error rate aware routing schemes perform significantly better than the vanilla scheme. Also, the choice between the routing strategies is clear. CER noticeably strains a satellite's energy reserves. However, when we consider both reliability and energy, the choice between the two strategies depends on the density of erroneous links present in the network. When erroneous links are sparsely present, CER exhibit a higher energy – reliability ratio, implying the energy costs outweigh the benefits. However, when a large percentage of links are erroneous, it has a lower energy-reliability ratio. In terms of throughput achieved, CER always delivers packets to ground stations at a rate lower than that of REL.

2.6 Datagram Transport Layer Security (DTLS):

TLS is most widely deployed protocol for securing network traffic. The primary advantage of TLS is that it provides a transparent connection oriented channel that is easy to secure an application protocol by inserting TLS between the application layer and transport layer. But, it cannot be used to secure unreliable datagram traffic. A solution is to minimize new security invention and to maximize the amount of code and infrastructure reuse for datagram i.e. to build TLS over datagram as the packets may be lost in datagram environment.[4]

The DTLS protocol is designed to secure data between communicating applications that run in application space without requiring kernel modifications. DTLS adds explicit state to the records to over come the inter-record dependency and uses simple retransmission timer and handles the re-ordering, replay detection. Also, the datagram packet sizes are often limited to less than 1500 bytes and this is overcome by Fragmentation and use fragment offset and specific fragment length.

2.7 SATELLITE GROUPING AND ROUTING PROTOCOL (SGRP)

This paper [13] presents a routing protocol, for hierarchical LEO/MEO satellite IP networks. SGRP operates on a two-layer satellite network consisting Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) satellites. LEO satellites are grouped according to the foot print snapshot of the MEO satellites. The LEO group members change as the MEO satellite moves. MEO satellite covering the LEO satellite group is taken as group manager. Link delay information is passed by the LEO satellites to their respective group managers. MEO satellites on receiving the link delay information, exchange with other MEO satellites and compute the routing tables for the LEO satellites.

SGRP aims at finding minimum delay paths for LEO satellites by sharing the routing table information with all the higher level MEO satellites. Load on the satellite system is assumed to be moderate. MEO satellites role in protocol is mainly confined to routing table calculation and transmission of signaling and data control packets. The exchange of delay information and routing tables among the intra orbit and inter orbit may result in extra overhead for the protocol. Energy constraints of the network are not addressed. The flat architecture can have multiple source destination routes to explore from, when compared with hierarchical architecture. In the flat tier architecture all the satellites have equal role in finding the routes.

CHAPTER III

METHODOLOGY

3.1 SYSTEM ARCHITECTURE:

Figure 1 shows a typical deep space network with several (S) nodes near to the ground station and several nodes (D) showing the root satellites. Here, the node S represents satellite that is one hop from the ground station on earth.

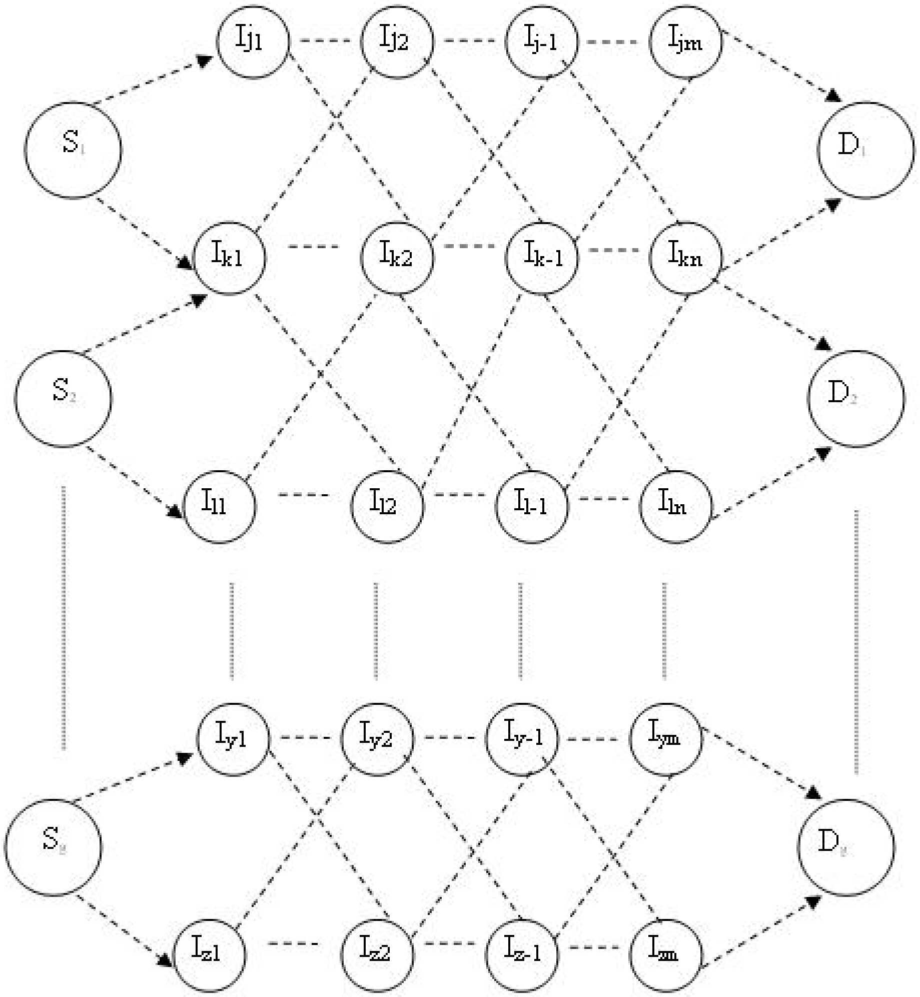

Figure 1: Typical deep space network

3.2 PROBLEM FORMULATION:

The main objectives of the proposed work are as follows:

a. Two nodes within a communication range R should be able to generate a key for secure communications i.e.

$$\begin{aligned} &\forall\, i, j \text{ such that distance}(i, j) \le R \\ &\qquad\qquad \Rightarrow \text{key\_share}(i, j) \end{aligned}$$

b. The path selected using the proposed approach will be optimal in terms of the energy distribution among nodes and the end to end delay in the path i.e.

$$\begin{aligned} &\max\Big(\sum_{i=1}^{n} \text{Energy}_{\,i} \quad \text{such that} \\ &\quad \min\Big(\sum_{j=1}^{n} \sum_{i=1}^{n} (\text{Energy}_{\,i} - \text{Energy}_{\,j}) \Big) \text{ and} \\ &\quad \min(\text{delay}(\ i, j))\ \forall\, i, j \end{aligned}$$

The proposed work provides a reliable channel for communication; the use of UDP will be encouraged rather than TCP. Moreover, we can vary the packet size to ensure maximum efficiency. This may be built on open technology such as SCPS [5] for easy upgrade of software in case there is a need to solve issues that might arise in the future. Furthermore, DTLS can be considered to improve efficiency [4]

In the proposed algorithm, every satellite in the network is termed a node and the node at destination/receiving end (satellite or space shuttle) is termed as the root node. Adjacent satellites can communicate with each other and share keys to enable secure communication without much overhead. During the initialization step, the algorithm generates a key graph from the physical graph with links between all possible nodes that can share a key. Here, the additional constraint on the network that differs from a traditional deep space network is that the nodes can communicate with another node within its communication range if and only if they can share a key. Unlike mobile networks, once the connection is established, they tend to exist unless the satellites move away from each other which will be for a definite period of time. The movement of satellite is pre-determined and hence the proposed algorithm supports the system.

All the nodes are assumed to have some form of unique ID’s from existing systems like CCSDS and this is used as reference for location based authentication. When they are deployed, this information can be used to localize them. Unlike the SGRP (LEO/ MEO) protocol, the LEO satellites not only measure the delay reports between them, but also focus on minimum energy consumption [5] and transmit this information to the node at a higher level, which transmits this to the ground station for computing the routing table information.

In the Link Activation Step [6], the algorithm discovers the shortest cost paths for each of satellites to a single branch root satellites using shortest path algorithms and in the load balancing step, the load is distributed across satellites in the constellation to avoid situations where a satellite is under-utilized or over-utilized.

3.3 Assumptions and Key Terms:

1. Each satellite is assumed to have good processing capabilities such as memory required or the processing capabilities of a complex network in order to perform computations. When the network is being set up, the individual nodes should be able to compute the keys.
2. The input is a random graph from the root nodes to the destination nodes with several possible paths from each node to every other node including the source and destination

Root nodes: The satellite at the destination/receiving side of communication when the system is setup.

Ground Station: These are half duplex nodes that are equipped with directional antennas and are fixed. They have more resources compared to satellites and are assumed to be homogenous in nature.

Mobile Satellites: Satellites rotate according to orbital kinematics and hence their motion can be pre-determined and the root satellites keep changing with time.

Physical Graph: A random graph with links between each of the nodes in the network defined as $G_p = (V_p, E_p)$ where V_p is a set of vertices in the physical graph and $E_p = (u, v) \mid u, v \in V$, u and v are connected by a physical link is the set of edges (links) in the physical graph.

Key Graph: The graph with details of satellites that share a common key space and is defined as $G_k = (V_k, E_k)$ where V_k is a set of vertices in key graph and E_k is the set of edges (links) in the key graph

RELIABILITY OF PATH: Reliability of the path is a measure of the total cost in a path. The total cost is a function of the delay between the links and the energy available at a node. This function is defined as Step 2.d of our algorithm as outlined in Section 3.5. We have higher reliability in the path if we select a path that has the lowest cost when compared to every other possible path in the network.

COST OF LINK: For every link, we compute the delay which is given as follows:

$$\text{delay} = \frac{\text{distance between nodes}}{\text{speed of light}} = \frac{\text{distance between nodes}}{\text{186000 miles per sec}}$$

The delay (which has units measured in time) is then normalized against the mean which is equal to 100 % and is termed as cost of a link

i. e. Cost of a link = (Actual Value / Mean) * 100

For example, the actual time is 100 ms and the mean is 50 ms, therefore the normalized value is 200. The normalized value thus obtained is independent of the units

ACCEPTABLE LOAD: Each satellite is assumed to have different load handling capacity. Some satellites are more advanced than other satellites so the load handling capacities of satellites vary. It is computed based on three factors:

1. Incoming bandwidth
2. Outgoing bandwidth
3. Processing Capability

Each satellite is assumed to handle a maximum incoming bandwidth (say MAX_IN_BW) and can transmit a maximum outgoing bandwidth at a time (say MAX_OUT_BW) and has processing capability (say PROCESSING_POWER). The Acceptable load of a satellite is given as follows:

$$\text{Acceptable Load} = \frac{MAX\_OUT\_BW}{\text{MAX\_IN\_BW}} * \text{PROCESSING\_POWER}$$

The acceptable load is then normalized against the mean which is equal to 100 %

i. e. (Actual Value / Mean) * 100

Capacity of Node: It is defined as the amount of energy resources that are available at a node for communication. We assume that a node has 100% of resources, so the capacity of a node is given by

Capacity of node = 100% - (% of energy consumed)

Cost of Node: This is a cost metric which is determined based on the capacity of node, acceptable load and the number of incoming channels. It is denoted as C (N_i).

For every node, we assign a cost which is given as follows:

$$\text{cost of node} \propto \frac{1}{\text{(capacity of node)(Acceptable Load)}}$$

$$\text{cost of node} = k\frac{1}{\text{(capacity of node)(Acceptable Load)}}$$

where k denotes the number of incoming channels.

The idea is that as the capacity of a node decreases, it reduces the reliability of a path, thereby increasing the cost of node. This helps us in selecting the nodes that improve the reliability of the path.

3.5 ALGORITHM

The input to the algorithm is a random graph as shown in figure 1.

Step 1: At each level, determine the nodes that can share key with neighboring nodes. All the nodes are assumed to have some form of unique ID's from existing systems like CCSDS and this is used as reference for location based authentication. This can be done as described in Location based authentication (Chapter 2.4) using Range free localization as each satellite acts as an anchor.

Step 2: After the previous step, we get a graph that is secure as each node shares key with its neighbors. Now, we compute the following at each node/link in the graph:

Step 2.a) Compute Acceptable Load for each node in the graph.

$$\text{Acceptable Load} = \frac{MAX\_OUT\_BW}{\text{MAX\_IN\_BW}} * \text{PROCESSING\_POWER}$$

Normalize the Acceptable Load against the mean as follows:

= (Actual Value / Mean) * 100 %

Step 2.b) Compute Cost of Node for each node in the graph as follows:

$$\text{cost of node} = k\frac{1}{(\text{capacity of node})(\text{Acceptable Load})}$$

where k denotes the number of incoming channels.

Step 2.c) Compute Cost of Link for every link in the graph as follows:

$$\text{delay} = \frac{\text{distance between nodes}}{\text{186000 miles per sec}}$$

Normalize the delay against the mean as follows:

Cost of Link = (Actual Value / Mean) * 100

Step 2.d) Compute new cost of links as follows:

New_Cost_on_Link [i] [j] = Cost_of_link[i][j] * Cost_of_node[j]

Here, Cost_of_link[i][j] denotes the link between node i and node j

New_Cost_of_link[i][j] denotes the link between node i and node j

Cost_of_node[j] denotes cost of node j

Step 3: After computing the new costs on the link, we apply Dijkstra’s shortest path algorithm to compute the shortest, secure and reliable path in the graph.

The first objective is that two nodes within a communication range R should be able to generate a key for secure communications is met by the algorithm as location based authentication guarantees that as long as two nodes are within the transmission range R, they can share a key. This provides us with a secure path.

The second objective is that the path selected using proposed approach will be optimal in terms of the energy distribution among nodes and the end to end delay in the path is met by the algorithm as the algorithm computes a shortest cost path. The cost here is assigned based on the capacity of node, number of incoming channels and the acceptable load at a satellite. These factors make sure that no node is overloaded i.e. the energy consumed is balanced equally across all the nodes in the graph. This makes the algorithm energy efficient and reliable.

Due to the simplicity of the algorithm, it can be implemented along with existing space based systems or can be used as stand alone. It can be used as stand-alone as it finds a path that is not only optimized in terms of its energy available at each satellite in the path but also on the distance between the satellites. Moreover, to have a path that has lower error rates, it can be integrated with the algorithm presented in [6].

SCPS was developed for reliable transfer of information between space mission end systems. As reliability is our main concern and as SCPS is built on open technology, integrating SCPS with the proposed algorithm will provide a higher reliability path for transfer of information.

CHAPTER IV

SIMULATIONS

A simulation program was written using JAVA. We assume that all the satellites have the same acceptable load. It is observed that the shortest path found is the optimal path from the source to destination in terms of security and reliability as it takes into consideration the capacity of node which is dependent on the amount of energy reserves and the cost of a link which is based on the distance between the nodes and the number of incoming channels. We perform the following simulations:

a) Effect of Cost of Node on Reliability of path

b) Effect of Cost of Link on Reliability of path

c) Compare the path selected by proposed algorithm to the path selected without using this scheme.

d) Compare the delay in path selected by the proposed algorithm to path selected without using this scheme.

e) Compare the average number of links in the path selected by the proposed algorithm to the path selected without using this scheme.

f) Compare the energy consumed by a path selected by the proposed algorithm to the path selected without using this scheme.

4.1 Effect on Cost of Node on Reliability:

$$\text{cost of node} = k\,\frac{1}{(\text{capcity of node})(\text{Acceptable Load})}$$

As the capacity of a node increases, the cost of the node decreases. Hence, the shortest cost path selected will have nodes with higher amount of resources available. Moreover, the cost of a node is dependent on the number of inputs links to a node, and thus leads to higher reliability in the path.

			Number of Input Nodes				
Used (%)	**Available (%)**	**Cost of Node**	**1**	**2**	**3**	**4**	**5**
10	90	0.1	0.1	0.2	0.3	0.4	0.5
20	80	0.05	0.05	0.1	0.15	0.2	0.25
30	70	0.033333	0.033333	0.066667	0.1	0.133333	0.166667
40	60	0.025	0.025	0.05	0.075	0.1	0.125
50	50	0.02	0.02	0.04	0.06	0.08	0.1
60	40	0.016667	0.016667	0.033333	0.05	0.066667	0.083333
70	30	0.014286	0.014286	0.028571	0.042857	0.057143	0.071429
80	20	0.0125	0.0125	0.025	0.0375	0.05	0.0625
90	10	0.011111	0.011111	0.022222	0.033333	0.044444	0.055556

Table 1: Table showing relation between Cost of node based on % of energy available and number of input links to a node

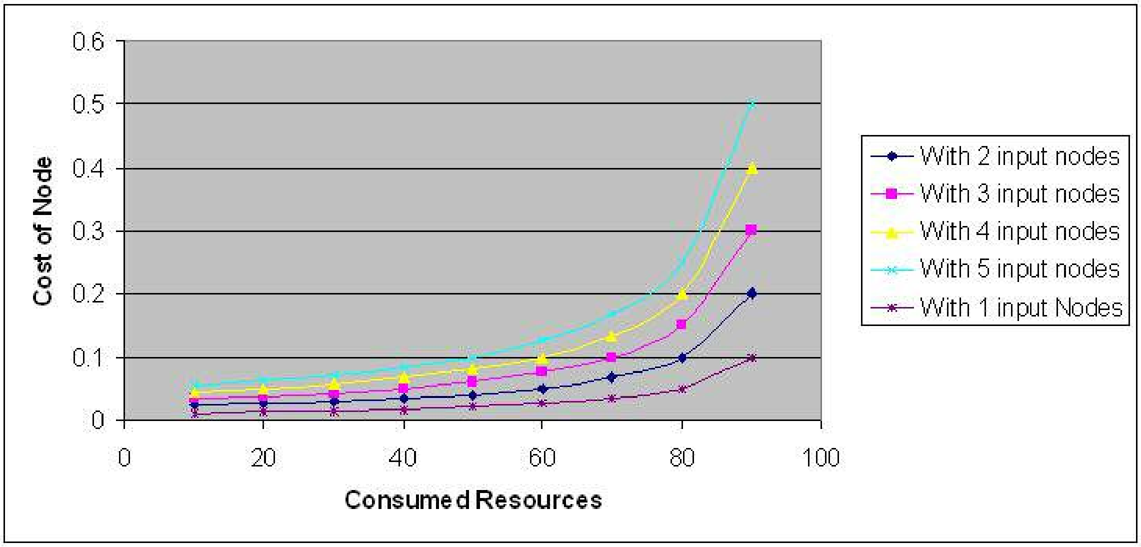

Figure 2: Chart showing relation between Cost of Node Vs Consumed resources

The graph shows that as the amount of consumed resources decreases, the cost of a node increases which is helpful to consider nodes that have higher energy resources available in the path with higher reliability. Moreover, the cost of node also increases as the number of incoming channels increases. The graph shows five different plotting showing the effect on cost of node as we increase the number of incoming channels from 1 to 5.

4.2 Effect on Cost of Link on Reliability:

$$\text{delay} = \frac{\text{distance between nodes}}{186000\ \text{miles per sec}}$$

As seen from the table, as the distance between the nodes increases, so does the normalized value and hence the smaller the probability that a link between two nodes with a shorter distance is chosen compared to a link between two nodes with larger distance is increased.

Distance	Value	Normalized Value
(miles)	(seconds)	
100000	0.537634	9.52381
200000	1.075269	19.04762
300000	1.612903	28.57143
400000	2.150538	38.09524
500000	2.688172	47.61905
600000	3.225806	57.14286
700000	3.763441	66.66667
800000	4.301075	76.19048
900000	4.83871	85.71429
1000000	5.376344	95.2381
1100000	5.913978	104.7619
1200000	6.451613	114.2857
1300000	6.989247	123.8095
1400000	7.526882	133.3333
1500000	8.064516	142.8571
1600000	8.602151	152.381
1700000	9.139785	161.9048
1800000	9.677419	171.4286
1900000	10.21505	180.9524
2000000	10.75269	190.4762
Mean =	5.645161	

Table 2: Table showing relation the distance between node and the normalized value assigned on the link

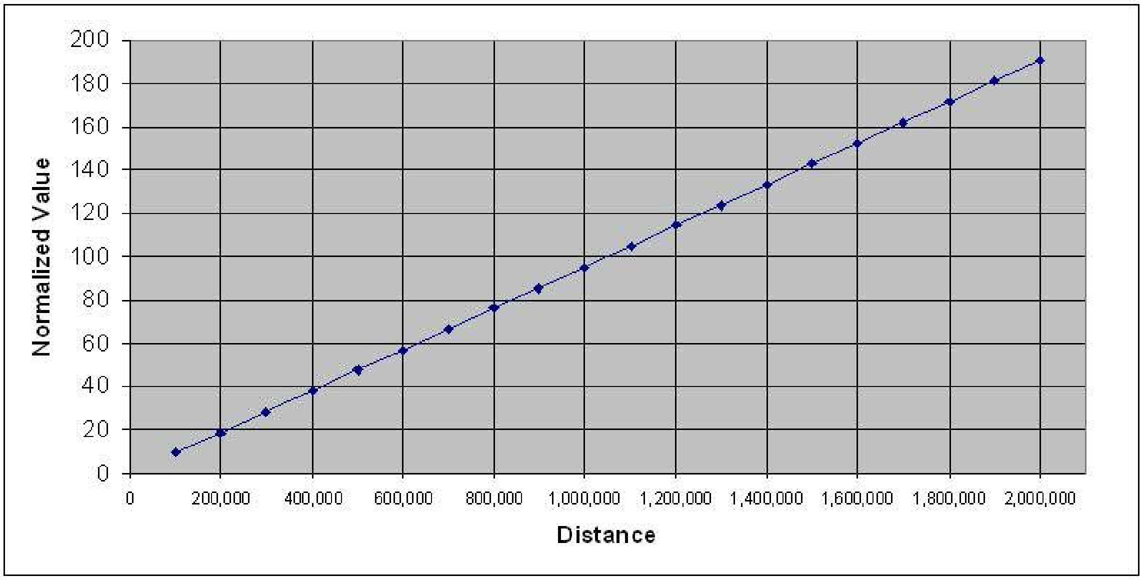

Figure 3: Chart showing relation between Cost of Link Vs the distance between nodes

The graph shows that as the distance between two nodes increase, the cost of link increases which is helpful in prioritizing links that are shorter compared to other links. Moreover, selecting a link which has lower cost helps in better signal quality and decreasing energy utilization to send the packet across the link.

4.3 Effect of Cost of node and Cost of Link on Path Selected:

Assume the following sample deep space network. For simulations, we assume that the each node has used 30% of its energy reserves and each node is at equidistant from every other node. So, the cost of each node is k/70 (k denotes number of input channels) and cost of each link is 100 (nodes are equidistant). We determine the path selected from this graph by using the proposed algorithm and compare with the path selected without using this approach.

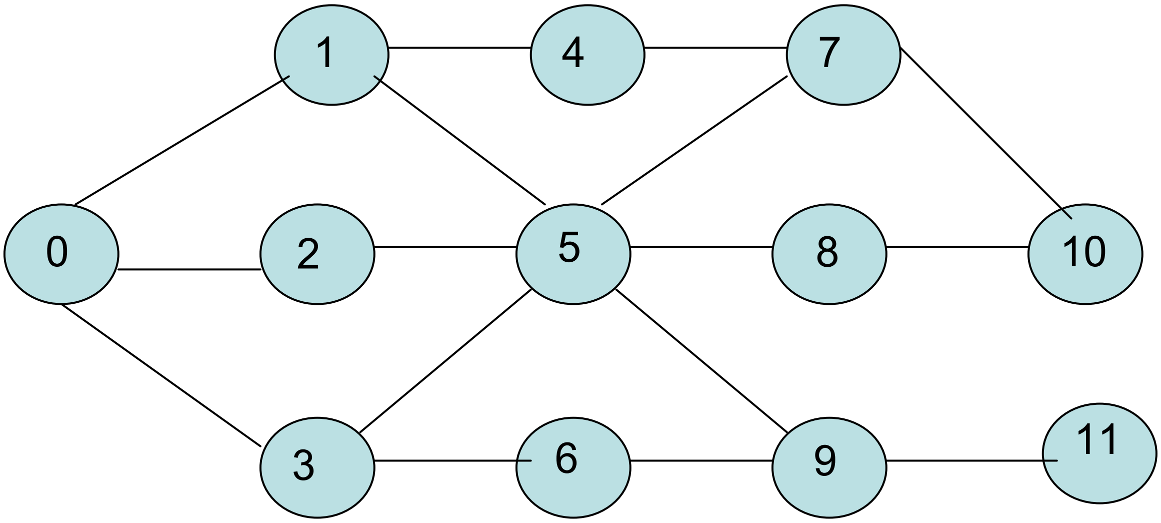

Figure 4: Sample deep space network

We apply the dijkstra’s shortest path algorithm as outlined in [14] for normal scheme considering only the delay in path. The possible paths from 0 to 10 are 0-1-4-7-10, 0-1-5-7-10, 0-1-5-8-10, 0-2-5-7-10, 0-2-5-8-10, 0-3-5-7-10 and 0-3-5-8-10. The possible paths from 0 to 11 are 0-1-5-9-11, 0-3-6-9-11 and 0-2-5-9-11. We observe that even though the cost of each node and link in the graph is same, our algorithm selects path 0-3-6-9-11 unlike the normal scheme which selects 0-1-5-9-11 to compute path between node 0 and node 11 even though they select the same path (0-1-4-7-10) between node 0 and node 10. This is because as node 5 has more incoming channels than node 3, so node 3 is selected (due to lower cost of node).

The reason that there is a difference between the path selected between node 0 and node 11 is because the normal scheme computes the shortest path (dijkstra's) from source to destination based on the delay on the link. So, when it tries to update distance by moving the nodes from Est to SP [14], we get 0-1-5-9-11 as the shortest path using a normal shortest path (dijkstra’s) scheme. But, when we use the proposed approach, it eliminates the presence of node 5 as it has lot of incoming links which increases the cost of node.

4.4 SIMULATION MODEL:

For further simulations we assume that all the satellites have used 30% of their energy reserves and have same acceptable load. The values taken for each network sizes of 10, 20 and 30 nodes are the average of 10 different topologies generated randomly.

The input to the algorithm is a pseudo-random graph that is generated using random links between source and destination nodes. This is different from a wireless ad hoc network as in a wireless ad hoc network any node can be source whereas in a satellite network there is a particular source and destination nodes. Moreover, the energy at each node in the network and the distance between any two nodes in the network is very higher in a satellite network when compared to a wireless ad hoc network.

The pseudo-random graph is generated by taking inputs as the total number of nodes in network, the number of source nodes and number of destination nodes. It then generates the distance and the presence of a link between two nodes using a random number generator. There are no links among the source nodes or the destination nodes. For instance, if the total number of nodes are 10 with two source and two destination nodes, then the source nodes are 0,1 and the destination nodes are 8, 9 and the nodes 2,3,4,5,6,7 are intermediate nodes.

We assume that 25% of the total nodes constitute the source and destination nodes i.e.

network of size 10 nodes has two source and two destination nodes, 20 nodes has four source and four destination nodes, and 30 nodes has six source and six destination nodes.

4.5 Comparison of Path Delays:

Path delay is the time taken (in seconds) for a packet to travel from source to destination node assuming that there are minimal overheads (equal to 0) at each satellite and that the packet travels at the speed of light(186000 miles per second) between two nodes as follows:

$$\text{path delay} = \frac{\text{total distance between all the nodes in a path}}{\text{186000 miles per sec}}$$

We compute the delay in path for different network sizes and take their average delay as shown below:

No of nodes	Proposed	Normal
10	4.311926	4.294808
20	3.357139	3.110189
30	3.287581	2.490238

Table 3: Table showing effect on delay using proposed scheme to without using the scheme

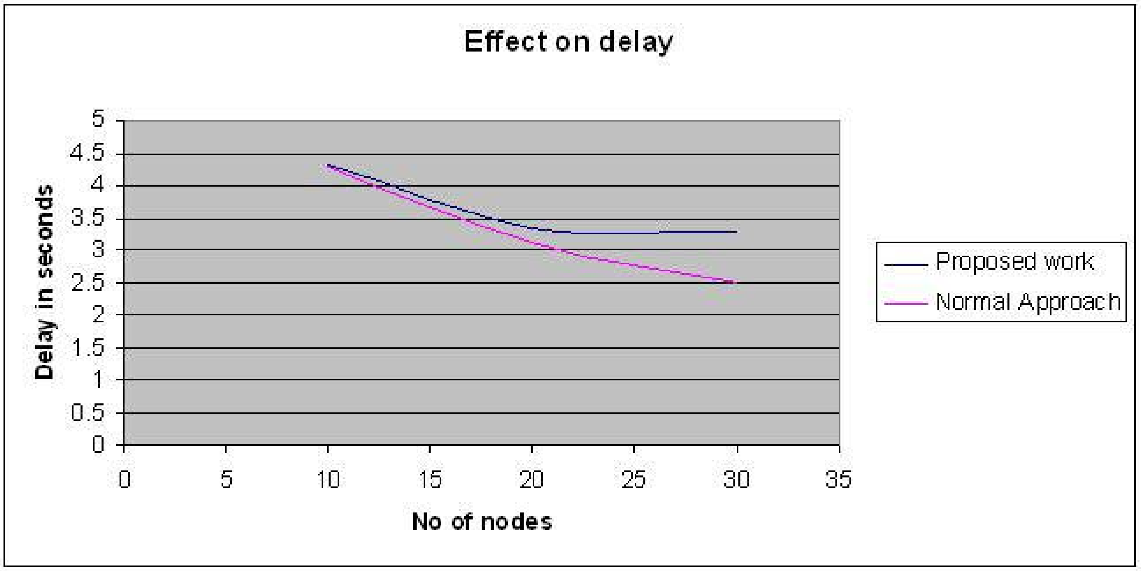

Figure 5: Chart showing effect on delay using proposed scheme to without using the scheme

As seen from the graph, the end to end delay is the same for a smaller number of nodes, but as the number of nodes increases, the end-to-end delay in the proposed approach is greater than the end-to-end delay in the normal approach.

4.6 COMPARISON OF AVERAGE PATH LENGTH:

Path length is the number of hops from source to destination node. For example, if the path is 0-4-5-9 then the number of hops is 3. We compute the number of hops in each path for different network sizes and take the average path length as shown below:

No of nodes	Proposed	Normal
10	2.272727	2.272727
20	2.545455	2.454545
30	3.0	2.818182

Table 4: Table showing effect on number of hops using proposed scheme to without using the scheme

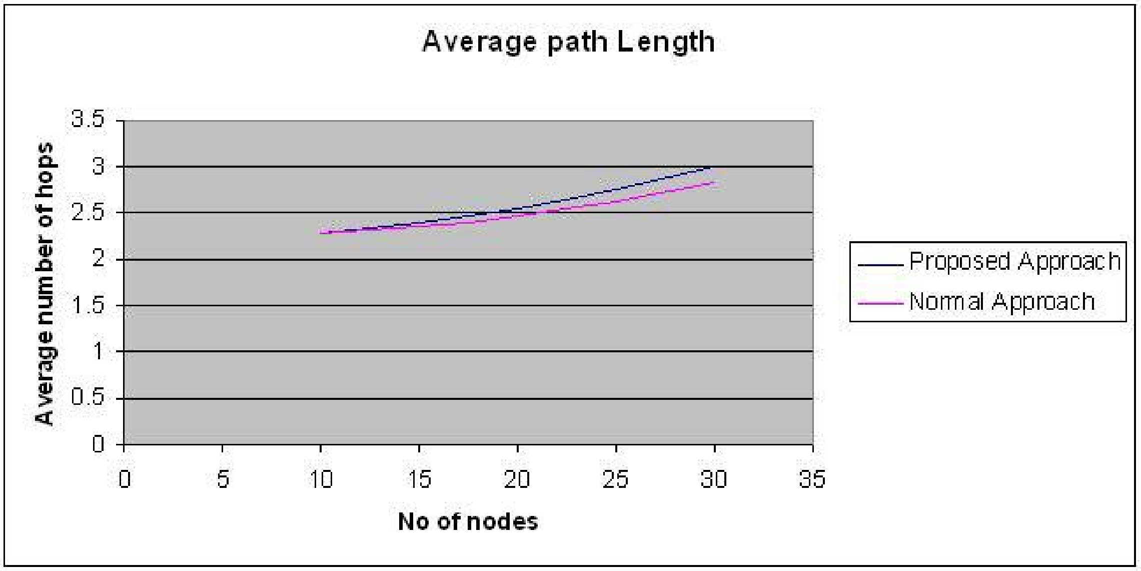

Figure 6: Chart showing effect on number of hops using proposed scheme to without using the scheme

As seen from the graph, the number of hops is almost the same for smaller number of nodes, but as the number of nodes increases, the number of hops in the proposed approach is greater than the number of hops in the normal approach.

4.7 Comparison of Average Number of Input Links:

The average number of input links in a path is the computed as follows:

$$\text{average number of input links in path} = \frac{\text{total number of links in path}}{\text{total number of nodes in path}}$$

Here, the total number of links in the path is the sum of total links through each node in the path. We compute the average number of input links in the path for different network sizes using proposed approach and without using this scheme as shown below:

Number of nodes	Thesis	Normal
10	2.583636	2.547273
20	5.213636	5.440909
30	8.036364	8.216667

Table 5: Table showing average number of links using proposed scheme to without using the scheme

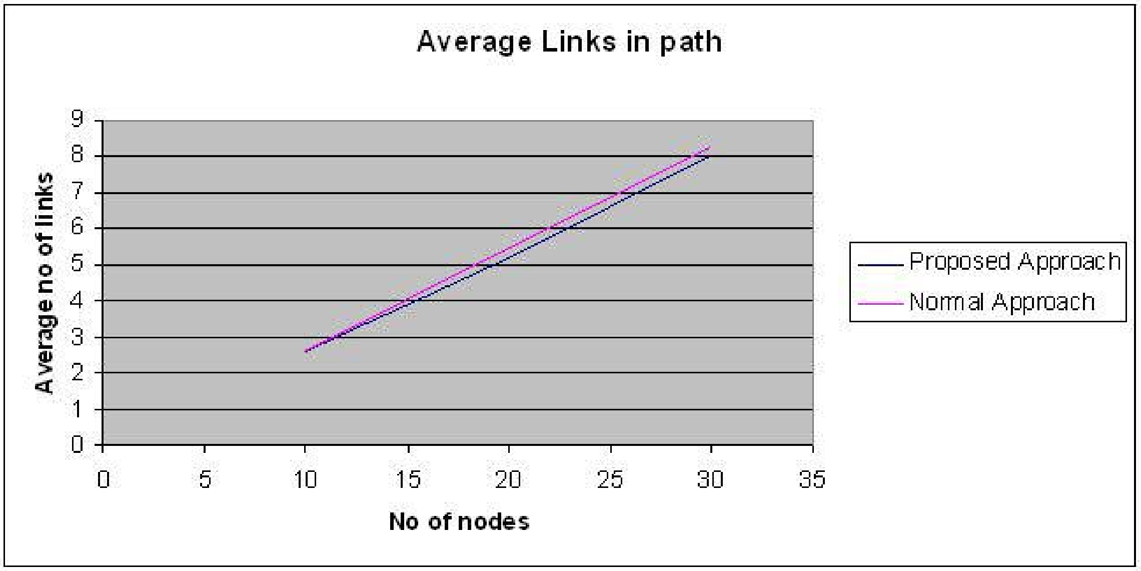

Figure 7: Table showing average number of links using proposed scheme to without using the scheme

As seen from the graph, the number of input links in the proposed approach is less when compared to the normal scheme. This helps in selecting nodes that might be less burdened in case all the potential links are active at once, thereby increasing the reliability of the path selected.

4.8 Comparison Of Energy Distribution:

After computing the shortest cost path, we assume that 10% of energy is consumed due to packet transmissions at each node. Also, if there is more than one path through the same node then the total energy at a node is divided equally for all paths. For example, if there are two paths that go through node k and that if node k has 90% of energy reserves left, then the total energy per path at the node k is 45%.

$$\text{Total energy in path} = \sum \text{Energy at each node in the path}$$

We compute total energy in path for different network sizes and take the average number of links as shown below:

No of nodes	Proposed approach	Normal approach
10	289.0	280.0
20	303.6364	276.3636
30	367.2727	285.4545

Table 6: Table showing comparing the energy left in a path using proposed scheme to the energy left without using this scheme

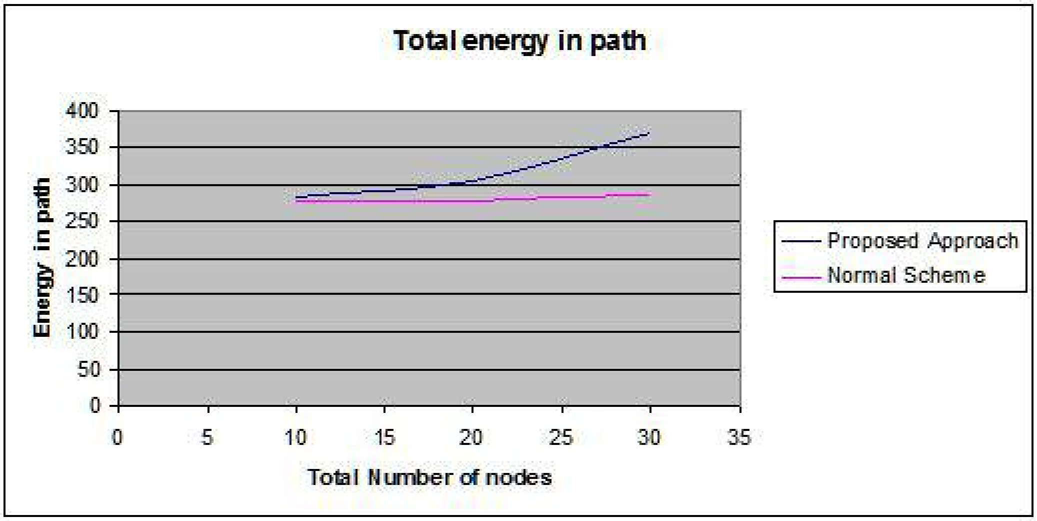

Figure 8: Chart showing comparing the energy left in a path using proposed scheme to the energy left without using this scheme

As seen from the graph, the energy remaining at the nodes selected in the path using our scheme is higher than the energy remaining at the nodes in the path selected without using our scheme. This implies that the energy reserves in a satellite are efficiently used in our algorithm and the algorithm minimizes the overload at any particular satellite.

As seen clearly, the reliability of the normal scheme is less than the reliability achieved using the proposed algorithm. (Here, reliability means that the nodes selected in the path have greater energy resources than other paths). Higher reliability is achieved as we are computing cost not only by the cost on a link, but also on the energy reserves of a node and the number of incoming channels. Also, this higher reliability is achieved with computations that are simple. With no added overhead to the existing system we can still achieve close to the same end to end delay. Moreover the proposed approach yields a secure path. Hence, this model is simple, secure and energy efficient.

CHAPTER V

CONCLUSION

Location based authentication enables deterministic, secure and efficient establishment of a shared key between two network nodes, be they immediate neighbors or multiple hops apart. The cost metrics assigned to nodes and links help us in determining the best possible path from source to destination in a deep space network, thereby selecting a path that has higher reliability than other paths. This has been observed by simulating the algorithm and measuring the effect of costs assigned to nodes and links during selection of the optimal path.

The proposed algorithm is simple, secure and energy efficient. The proposed algorithm provides an improved layer of security and increased reliability in the path through which sensitive data can be transferred. It has been noted that the topology of a satellite changes at regular time intervals and as this algorithm computes the shortest path without much overhead, it can be used for secure and reliable deep space communication.

The proposed work can be further improved by integrating it with the scheme proposed in [6] which provides stable load balancing with ground stations and increases reliability in the path by reducing loss of packets. It can also be further improved to reduce end to end delay.

REFERENCES

[1]. K Hogie, E Criscuolo, R. Parise, “Using Standard Internet protocols and applications in space” (2005) Computer Networks, 47 (5), pp. 603-650, 2005.

[2]. L P. Clare, J L Gao, E H Jennings, C. Okino, “Space based multi hop networking”, Computer Networks, Volume 47, Issue 5, Pages 701-724, 5 April 2005.

[3]. M. Yang, J. F. Ru, X.R. Li, H. Chen and A. Bashi, "Predicting Internet End-to-End Delay: A Multiple-Model Approach" in Proc. of IEEE INFOCOM 2005, Vol. 4, pp. 2815-2819 , Miami, Mar. 2005.

[4]. Modadugu,N.,Rescorla,E.,"The Design and implementation of Datagram TLS", Proceedings of Network and Distributed System Security Symposium, Internet Society 2004, Feb2004.

[5]. Robert D., Space Communications Protocol Standards Overview, http://www.scps.org/Documents/SCPSoverview.PDF [Date of last access 17 July 2007]

[6]. Vamsi MaramReddy, Osazuwa Amadasun, Venkatesh Sarangan, and Johnson Thomas, “Routing in Deep-space networks with lossy links” , 2007 IEEE Aerospace Conference, pp. 1-10, March 2007.

[8]. Consultative Committee for Space Data Systems, Space Communications Protocol Specification (SCPS)—Rationale, Requirements, and Application Notes, CCSDS 710.0-G-0.4, August 1998, http://bongo.jpl.nasa.gov/scps/Documents/GB04c.PDF [Date of last access 17 July 2007]

[9]. Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS-SP). Blue, http://public.ccsds.org/publications/SIS.aspx, [Date of last access 17 July 2007].

[10]. W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," ACM Transactions on Information and System Security, vol. 8, no. 2, pp. 228-58, May 2005.

[11]. M. Penrose, "On k-connectivity for a geometric random graph," Wiley Random Structures and Algorithms, vol. 15, no. 2, pp. 145–164.

[12]. "The recent Advances of Satellites", http://www.stmary.ws/physics/97/NBLANCAT.HTM [Date of last access 17 July 2007]

[13]. Ekylem Ekici, "A Routing Protocol for Hierarchical LEO/MEO Satellite IP Networks", Wireless Networks, Vol. 11, pp. 507-521, 2005.

[14]. "Dijkstra's Shortest Path Algorithm", http://www.math.grinnell.edu/~rebelsky/Courses/CS152/98S/Outlines/outline.50.html [Date of last access 17 July 2007]

VITA

Vinay Kumar Abburi

Candidate for the Degree of

Master of Science

Thesis: SECURE AND RELIABLE DEEP SPACE NETWORKS

Major Field: Computer Science

Biographical:

Personal Data:

Gender:	Male
Address:	70 S, University Place, Apt 2, Stillwater, OK 74075
Contact Number:	405 334 8162
Email address:	a.vinaykumar@gmail.com

Education:

1. Completed the requirements for the Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma in July 2007.
2. Bachelor of Engineering in Computer Science at Sri Nandhanam College of Engineering and Technology affiliated to Anna University, Chennai.
3. Vocational Course in Computer Science Engineering at Little Flower Junior College affiliated to Board of Intermediate Education.

Experience:

1. Website Development Intern, Teen emPower! Inc, Oklahoma City
2. Graduate Research Assistant, BAE, Oklahoma State University
3. Graduate Research Assistant, CS, Oklahoma State University

Professional Memberships:

1. Member of Golden Key International Honor Society, Oklahoma State University
2. Member of Association for Computer Machinery

Name: Vinay Kumar Abburi Date of Degree: December, 2007

Institution: Oklahoma State University Location: Stillwater, Oklahoma

Title of Study: SECURE AND RELIABLE DEEP SPACE NETWORKS

Pages in Study: 56 Candidate for the Degree of Master of Science

Major Field: Computer Science

Scope and Method of Study: Satellite systems have the advantage of global coverage and inherent broadcast capability and offer a solution for providing broadband access to end users. The main thrust of space communications to-date has been to provide reliable communications between ground mission control and a single spacecraft. Little work has been reported on developing a secure as well as a reliable mode of communications in a deep space satellite network. The main objective is to develop an algorithm that can increase the reliability (such as in terms of minimum energy consumption) and security in the communications path while minimizing overheads.

Findings and Conclusions: Location-based authentication is applied and costs assigned to every node and link in the path. The proposed approach then optimally selects path with the lowest cost that is also secure. We have developed an algorithm to efficiently compute a secure and reliable communications path at minimum cost. The proposed approach is compared to a shortest path approach. Simulation results indicate that although the proposed approach yields slightly longer paths, it provides a more efficient approach in terms of energy distribution as well as secure paths

ADVISER’S APPROVAL: Dr. Johnson Thomas