International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

NETWORK ADMINISTRATION USING THE ARMED FORCES OF COMPLEX ORIENTED COMMUNICATION PROTOCOLS

[*1]Ms. Prema G, [*2] Mrs. Archana D.

*[*1]Assisant Professor, PG & Research Department of Computer Science & Information Technology*

Arcot Sri Mahalakshmi Women's College, Vilapakkam, Vellore, TamilNadu, India.

*[*2] M.Phil Research Scholar, PG & Research Department of Computer Science & Information Technology*

Arcot Sri Mahalakshmi Women's College, Vilapakkam, Vellore, TamilNadu, India.

Abstract - ***In widely distributed systems generally, and in science-oriented Grids in particular, software, CPU time, storage, etc., are treated as "services" – they can be allocated and used with service guarantees that allows them to be integrated into systems that perform complex tasks. Network communication is currently not a service – it is provided, in general, as a "best effort" capability with no guarantees and only statistical predictability In order to obtain a highly reliable communications system, the development approach in terms of both services and protocols, must be suitably supported by appropriate specification tools that are able to provide complete, unambiguous and flexible description techniques. In most of communication applications the LOTOS language, among the standard formal description techniques, is widely used. An object oriented analysis is introduced to describe a specification method that can increase the specification accuracy while at the same time providing an efficient means for rapid prototyping. The article also shows the results of the proposed approach and describes a specific communication protocol, the controller area network (CAN), which is now being used in a broader class of applications within the factory automation process***

Key Words: *controller area network (CAN)*

I. INTRODUCTION

Network management, in general, is a service that employs a variety of protocols, tools, applications, and devices to assist human network managers in monitoring and controlling of the proper network resources, both hardware and software, to address service needs and the network objectives.

When transmission control protocol/internet protocol (TCP/IP) was developed, little thought was given to network management. Prior to the 1980s, the practice of network management was largely proprietary because of the high development cost. The rapid development in the 1980s towards larger and more complex networks caused a significant diffusion of network management technologies. The starting point in providing specific network management tools was in November 1987, when Simple Gateway Monitoring Protocol (SGMP) was issued. In early 1988, the Internet Architecture Board (IAB) approved Simple Network Management Protocol (SNMP) as a short-term solution for network management. Standards like SNMP and Common Management Information Protocol (CMIP) paved the way for standardized network management and development of innovative network management tools and applications.

A network management system (NMS) refers to a collection of applications that enable network components to be monitored and controlled. In general, network management systems have the same basic architecture. The architecture consists of two key elements: a managing device, called a management station, or a manager and the managed devices, called management agents or simply an agent.

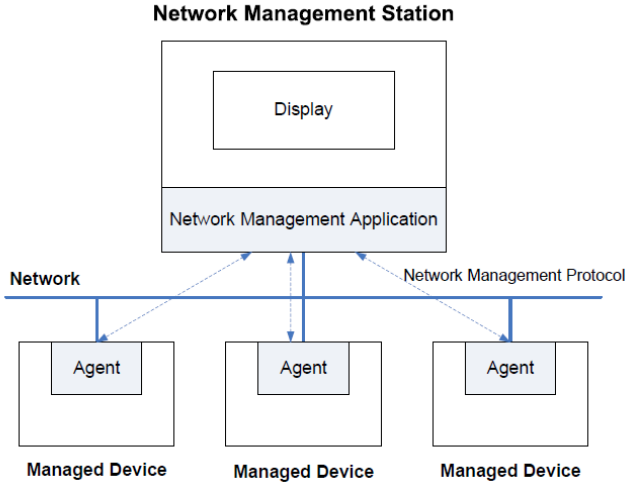

Fig: 1.1 Typical Network Management Architecture

1.2 OSI Network Management Model

1.2.1 The OSI network management comprises four major models:

- **Organization Model** defines the manager, agent, and managed object. It describes the components of a network management system, the components' functions and infrastructure.
- **Information Model** is concerned with the information structure and storage. It specifies the information base used to describe the managed objects and their relationships. The Structure of Management Information (SMI) defines the syntax and semantics of management information stored in the Management Information Base (MIB). The MIB is used by both the agent process and the manager process for management information exchange and storage.
- **Communication Model** deals with the way that information is exchanged between the agent and the manager and between the managers. There are three key elements in the communication model: transport protocol, application protocol and the actual message to be communicated.
- **Functional Model** comprises five functional areas of network management, which are discussed in more detail in the next section.

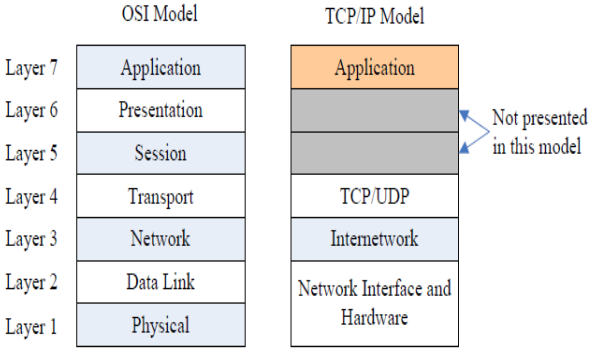

Fig: 1.2 The OSI and TCP/IP Reference Models

1.3 Definition - Network Management

Network Management is the act of initializing, monitoring and modifying the operation of the primary network functions. Primary network functions are those functions that directly support the user requirements. They allow for example users to access the network and they take care of the exchange of user data. During the design phase, the primary architectural concepts architectural rules architectural models As it was globally accepted that management involves the planning, organizing, monitoring, accounting, and controlling of activities and resources. This definition can certainly be applied to Management of the Network. The OSI and Internet Network Management Structures are focused principally on monitoring, accounting, and controlling Network management, those of planning and resources.

1.4 Fault handling

During a network's operational phase failures can occur suddenly. Failures are situations in which network components (or systems) do not behave in the way that has been specified. As a result of failures, networks may no longer provide the required service and it may even come to a complete breakdown. The occurrence of failures can be due to ageing and decay of network components (hardware), as well as to human errors (e.g. a dragline that accidentally breaks a cable).

1.5 Flexibility

Network designs are commonly described as top-down processes. Characteristic for such processes is the important role of user requirements; the design usually starts with the definition of the user requirements and many design decisions follow from these requirements.

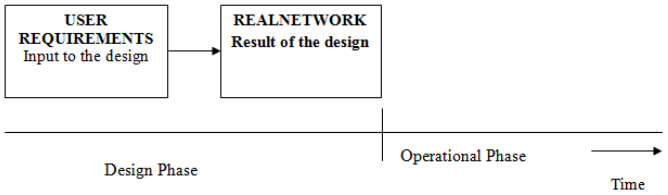

Figure 1.3: Simplified top-down design process

II. RELATED WORK

In the Management of Networks many companies operate in a heterogeneous environment and use a wide variety of hardware components, as well as different types of communications protocols. Organizations are faced with the formidable technical problem of building unique interconnection packages for each of their customer's vendor specific systems. The picture will only become more complex as voice and data networks grow within and between organizations. As client, customer, and vendor relationship grow, different interface and protocol supports will be needed.

2.1 IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organization which, amongst others, defines standards for Local and Metropolitan Area Networks (LANs and MANs). These standards are commonly known as the IEEE 802 standards. Some of these standards define how management should be performed in LAN and MAN environments

Number	Title
IEEE802.1B	LAN/WAN Management
IEEE 802.1E	System Load Protocol
IEEE802.1F	Common Definitions and Procedures for IEEE 802 Management Information.

Table 2.1 IEEE Management Standards

The Networking group (NET) of WICS focusing mainly on "Future Wireless Internet" consists of three teams: Networking, Future Wireless Internet and Sensor Network Architectures, and Sensor Networking. The group carries our research in the field of 5G/6G network architectures, spectra management, networks economics and security, as well as the future Internet applications

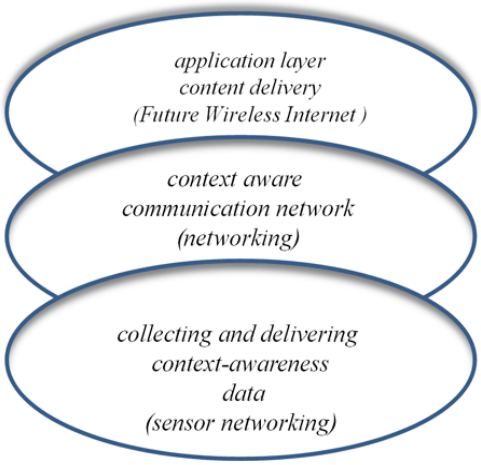

Figure: 2.1 Research focus of the Networking research group

2.2 Network Management Forum

In 1988 the 'OSI/Network Management Forum' was formed to promote the rapid development, acceptance and implementation of OSI and CCITT management standards. The Forum is a non-profit organization whose members are manufacturers, operating companies and research laboratories. After a few years the prefix 'OSI' was removed to indicate that the Forum had widened its scope to reference management standards from other sources.

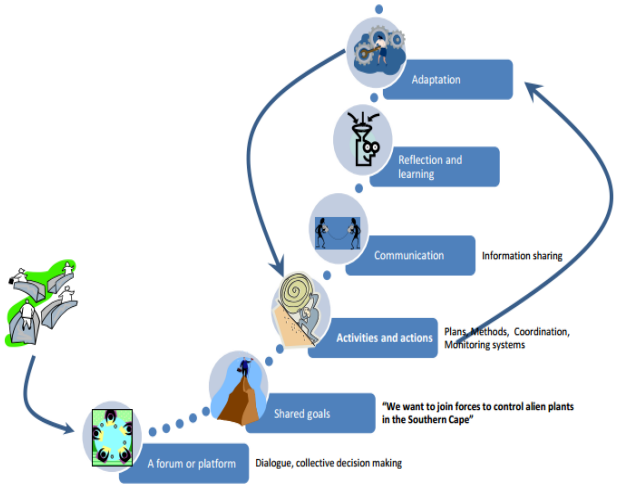

Fig: 2.2 Network Management Form

- SNMP from the IETF.
- The 'Distributed Management Environment' (DME) from the Open Software Foundation (OSF).
- The 'Management Protocol API' (XMP) and the 'OSI-Abstract Data Manipulation API' (XOM) from X/Open.
- The 'Common Object Request Broker Architecture' (CORBA) from the Open Management Group (OMG).

2.4 Need for the Network Management Standards

As the Network uses too many components of different architecture and makes when we are not using the Network Management Standards the problem of interface between two networks of different Architecture arises which leads the cost to develop and maintain these interface systems can be extraordinary, often resulting in complex software and unpredictable performances and may lead to the failure of the Network System.

2.5 Integrated Network management

As we discussed earlier that the main aim of this research is to support an integrated approach to the management of a Network (or networks) which contains multi-user computers, software packages, and carriers. The following are the key points that we are going to study about Integrated Network Management:

- Integrated Network Management is needed to reduce the cost of interfacing different systems.
- Network Management requires uniformity in the exchange of management information between different user's product lines.
- Integrated Network Management is needed so that basic level of management service is the same for all i.e Network performance, accounting, configuration security and fault criteria, and the exchange of common protocol data units.
- Integration and uniformity does not produce value-added services within the context of these standards.

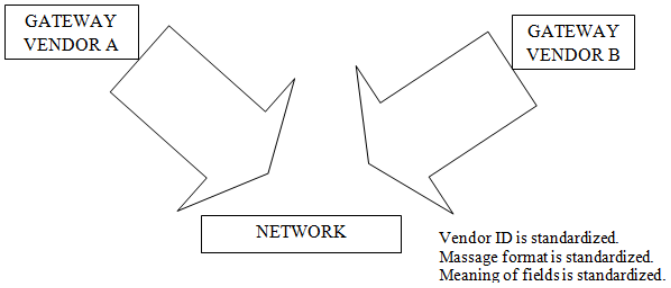

Figure: 2.3 Using Standardized Network Management Protocols

III.COMPONENTS OF NETWORK MANAGEMENT

3.1 Components of Network Management

The OSI, Internet, and IEEE Network Management Standards define the responsibility for a managing process (called a Network Management system in some vendors products) and a managed agent (also known as an agent process). In the simplest sense, a Network Management system really contains nothing more than protocols that convey information about Network elements back and forth between various agents in the system and the managing process.

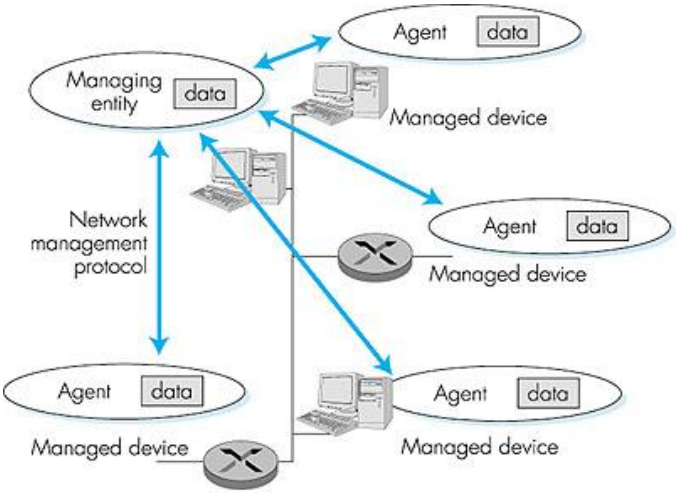

Figure 3.1 Network management

The managing entity is an application, typically with a human in the loop, running in a centralized network management station in the network operations center (NOC). The managing entity is the locus of activity for network management; it controls the collection, processing, analysis, and/or display of network management information. It is here that actions are initiated to control network behavior and here –[that the human network administrator interacts with the network devices.

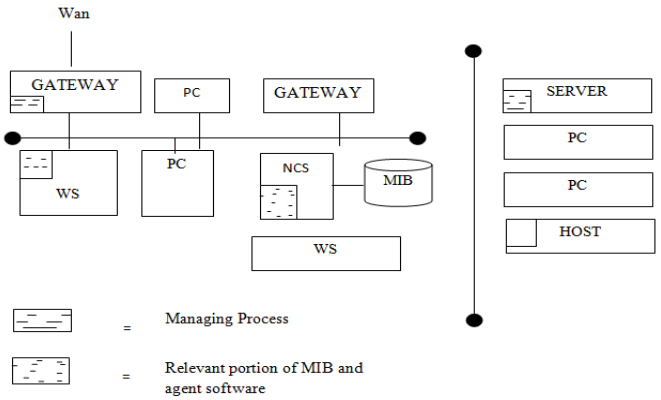

Fig: 3.2 Components of Network Management System

3.2 Object-Oriented Design

The concept of OOD was first originated in the early 1970s. The OSI Network Management Standards in Open System Interconnection uses many concepts of OOD. The Internet and IEEE model also uses OOD concepts. The notion of an object as a construct for manipulation (in effect, a programming construct) was first found in Simula, which a language was used to program computer simulations.

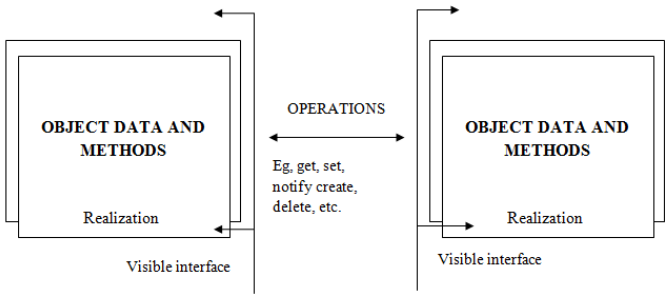

Figure 3.3 objects oriented design concepts

3.2.1 Finally, dynamic inheritance is further divided as:

Part Inheritance

Part inheritance systems allow an object to change its behavior by receiving operations from other objects. With OSI Network management, this means that the messages are passed to the managed objects, which we have learned, is also called external stimuli.

Scope inheritance

In contrast, scope inheritance establishes that an object behavior is determined by its environment and may be altered by its environment. In OSI Network management, this idea is referred to as internal stimuli.

Polymorphism

The concept of polymorphism and class is the key to building a reusable system, because such an approach makes it possible to build generic software logic which can be applied to a wide range of managed time.

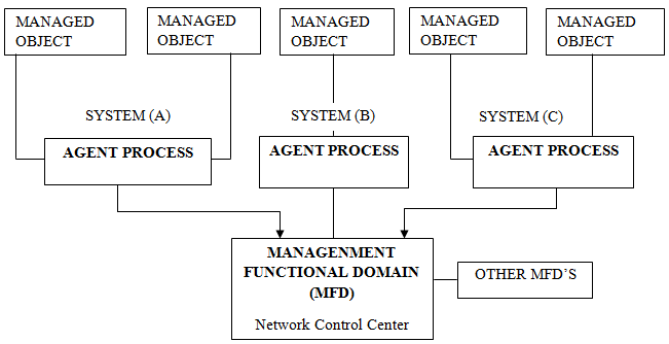

Fig 3.4 Managed objects under Object oriented design

From the OSI perspective, managed objects are classified by how they fit into the OSI layers. If they are specific to an individual layer, they are called (N)-layer-managed objects. If they pertain to more than one layer, they are called system-managed objects.
The other aspects of managed objects are:

The permissible management operations that can be performed on a managed object must from part of its definition.

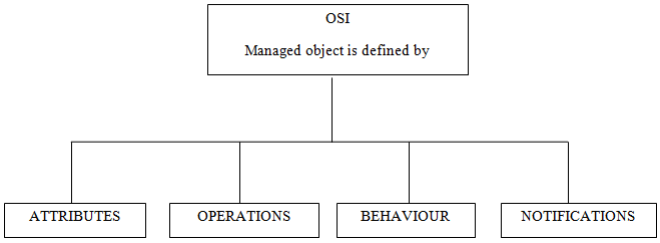

Figure: 3.5 How Managed Objects Are Defined

- The definition of a managed object may also include the effect that these operations have on related system resources.
- The state of the managed object or its properties may determine the type of operation that can be performed on the managed object.

IV. OBJECT ORIENTED FRAMEWORK, CMIP/CMIS PROVIDES SERVICES

A central concept to understanding the operation of TMN is found in the area of object-oriented systems. For those of you come from a Computer Science background with significant exposure to object oriented systems, the concepts are very similar with some slight deviations in terminology. If you only have limited exposure to object oriented design and concepts, any foray into the world of TMN should probably be preceded with some study of object oriented design disciplines. A growing set of resources can be found in the literature. Information on Object Oriented design techniques is available from sources such as Booch, Rumbaugh and others. For getting a more complete description of the object oriented concepts as they apply to CMIP, Stalling's book on SNMP, SNMPv2 and CMIP contains a good section describing the nature of the concepts.

4.1 Organizing the Objects - Multiple Relationships

As in any data intensive system, information must be maintained in some schema with which users (typically management systems) can access the information. Within the OSI management schema, there are three types of relationships between managed objects, including:

- Inheritance Tree - defines the managed object class super and sub-classes, much as C++ base and derived classes are related.
- Containment Tree - defines which managed objects are contained in other managed objects.

4.2 CMIP - Common Management Information Protocol

Access to managed information in the managed objects is provided by the Common Management Information Service Element (CMISE) that uses CMIP to issue requests for management services. The management services provided by CMIP/CMISE can be organized into two distinct groups, management operation services initiated by a manager to request that an agent provide certain services or information, and notification services, used by the management agents to inform the managers that some event or set of events have occurred.

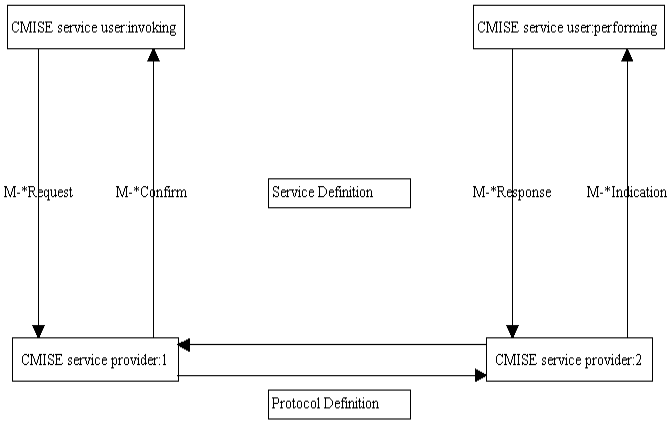

Figure 4.1 CMIP Protocol

CMISE requests can be scoped to apply to a range of managed objects. Four levels of scoping can be applied, with the request being applied to:

- The base object (as identified by the Distinguished Name)
- Objects at the *nth* level subordinate to the object. The base object is termed to be at level 0 for this type of scoping
- The base object and all managed objects to (and including) the *nth* level
- An entire subtree - the base object and all subordinate objects on the containment tree

V. OSI OBJECT CLASSES AND INTERNET GROUPS

In OSI model, managed objects that have similar characteristics are grouped into an object class, which is called a Managed Object Class (MOC). In OSI, the characteristics used to determine object classes are attributes, operations, and notifications. MOCs provide a convenient means to group related resources together. This means that it is possible to encapsulate (or contain) objects within other objects and, in so doing, invoke operations or receive notifications only on the relevant "layer" of the encapsulated objects.

As we discussed earlier that a management process manages the managed objects, which is an application process. As shown in figure 1.8 the management process is categorized as

1. **A managing process** A managing process is defined as part of application process that is responsible for management activities.
2. **An agent process**. An agent process performs the management functions on the management objects at the request of the managing process.

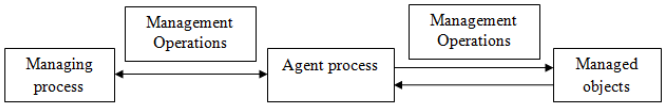

Figure 5.1 OSI management processes

5.1 The Functional Component

This component describes the various activities to be performed in support of management. X.700 has grouped the management functions into five areas. These are configuration, fault, performance, security, and accounting management.

5.2 The Information Component

Management information exchanged between the managing and managed systems is dependent on both the function to be performed as well as the resources3 to be managed. A major thrust of OSI systems management is to model the resources being managed.

5.3 The Communication Component

The third dimension of facilitating a successful management interface between the roles of managing and managed systems is to have a well defined structure for the systems management protocol. The goal is to enable successful transfer and interpretation of management information. Communication

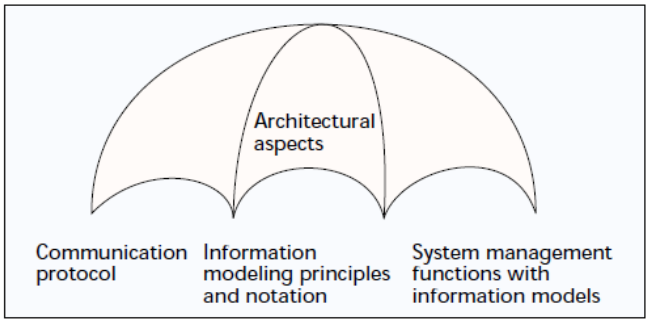

Figure: 5.2 Architectural Aspects

VI. EVALUATION RESULT:

The AODV protocol performance was evaluated with the "Network Simulator 2" (ns–2), which is one of the most powerful tools used to simulate wired and wireless network protocols. For our case of study, three simulation scenarios were considered: in the first one the simulation was carried out in normal conditions, in other words, all the nodes participated correctly in the routing functions. In the second scenario, one of the nodes was a malicious node which accomplished the sequence number attack. In the third scenario, an attack detection module was proposed and it was incorporated in the AODV protocol and simulated again.

The metrics that we used to evaluate the attack detection module performance are the following: (1) Packet delivery ratio or percentage (considered as our most important metric), (2) Number of RREP packets sent by node number 2 (the malicious node), (3) Accuracy on attack detection, and (4) Average latency of the transmitted packets.

6.1 Throughput

We have measured end to end throughput in Kbits/sec for each source destination pair over both the network scenarios. A high individual and average throughput is observed in all the cases by the modified protocols. The result obtained can be attributed to the fact that due to the selection of the path having highest SNR value the impact of interference and jamming signals are less and path bandwidth is increased which is reflected as higher throughput that is desirable for almost every envisaged application of MANET. A considerable improvement in average throughput is observed in both the scenario for all routing protocol

End-to-End Delay (In Sec)	52 Nodes Scenario	72 Nodes Scenario
OLSR-INRIA	0.818	0.727
SOLSR-INRIA	0.329	0.131
DSR	01.48	1.404
SDSR	0.178	0.235
ZRP	0.185	04.04
SZRP	0.126	0.171

Table 6.1 Throughput

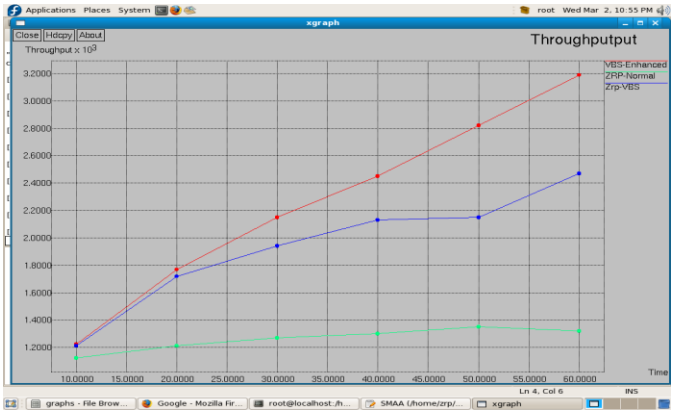

Figure 6.1: Throughput

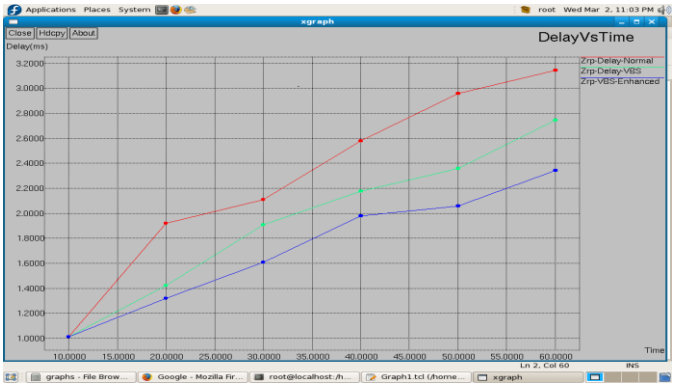

Figure 6.2: Delay Vs Time

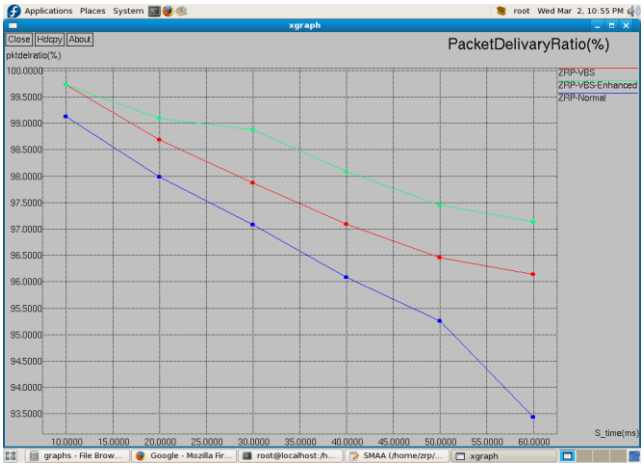

Figure 6.3: Delivery Ratio

CONCLUSION

From the simulation results it can be concluded that for SOLSR-INRIA, SDSR and SZRP average throughput increases while average end-to-end delay and jitter decreases considerably as compared to OLSR-INRIA, DSR and ZRP in both the scenarios. The modified protocols avoid malicious nodes and noisy links by choosing the highest SNR path which increases overall network reliability. Random Waypoint (RWP) mobility model is considered as it encompasses most of the envisaged application areas of Network. We have extensively simulated our methods using QualNet 4.5 network simulator. As a future work other mobility models and data traffic might be considered. Intrusion detection methods may be incorporated in the route discovery phase of OLSR-INRIA, DSR and ZRP for detection of malicious nodes to enhance network reliability.

In this thesis, I have implemented two secure routing protocols, OLSR and SAODV, based on their respective underlying protocols, DSR and AODV, in the OPNET simulation environment. I have also simulated four popular network attack models that exploit the weakness of the protocols. The attack models are used to make malicious wireless nodes and create various malicious environments, in which the performance of DSR, AODV, OLSR, and SAODV are evaluated. With three different attack models for each of the protocols, and with the number of malicious nodes varying from one to five, totally 65 scenarios are created to evaluate the four protocols.

The ultimate goal of a routing protocol is to efficiently deliver the network data to the destinations; therefore, two metrics, Packet Delivery Fraction (PDF) and Normalized Routing Load (NRL), are used to evaluate the protocols. In order to get the accurate experimental results, each scenario is run eleven times in order to calculate the average value for the two evaluation metrics. Through the collected evaluation metrics from the various scenarios, the impacts of attacks upon the routing protocols are then studied.

Future Research

- The OLSR protocol needs to be improved in order for the cached route feature to be secure and effective in malicious environments.
- A public key verification mechanism, such as certificate-based authentication, is needed for SAODV, in order to verify the binding between the node's identity and its public key.

More research is needed in the mobility of the nodes in order to comprehensively evaluate the impact of the malicious nodes' movement on the protocol's performance.

REFERENCES:

1. T.H Clausen, G.Hansen, L.Christensen, G. Behrmann, " The Optimised Link State Routing Protocol Evaluation Through Experiments and Simulations", Proceedings of IEEE Symposium on Wireless Personal Mobile Communications, 2001, September 2001.
2. D.B Johnson, D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, Kluwer Academic Publishers, 1996, vol. 353, pp. 153-181.
3. D. Sivakumar, B. Suseela, R. Varadharajan, "A Survey of Routing Algorithms for MANET", IEEE International Conference on Advances in Engineering, Science and Management (ICAESM), March 30-31, 2012, pp. 625-640. Available in IEEE Explore.
4. V.Jha, K. Khetarpal, M.Sharma, "A Survey of Nature inspired Routing Algorithms for MANETs", IEEE 3rd International Conference on Electronics, Computing Technology (ICECT), April 8-10, 2011, pp. 1-4. Available in IEEE Explore.
5. S.Weber, J.G Andrews, N. Jindal, "An Overview of Transmission Capacity of Wireless Networks", IEEE Transactions on Communication, vol. 58, Issue. 12, 2010, pp. 3593-3604.
6. Royer E M, Toh C K, "A review of current routing protocols for Adhoc mobile wireless networks" IEEE Journal of Personal Communications, Dec. 2006, vol. 6(2), pp. 46- 55.
7. Z.J Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks", Proceedings of ICUPC 1997, vol. 2, pp. 562-566, October 1997.
8. P. Nand, and S.C. Sharma, "Performance study of Broadcast based Mobile Ad hoc Routing Protocols AODV, DSR and DYMO", Proc. International Journal of Security and Its Applications, Vol. 5, No. 1, January, 2011, pp. 53-64.
9. D.B. Johnson, D.A. Maltz and J. Borch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Computer Science Department Carnegie Mellon University Pittsburgh, PA15213-3891, Dec. 2009. http://www.monarch.cs.cmu.edu.
10. J. Liy, H. Kameday and Y. Panz, "Study on Dynamic Source Routing Protocols for MANET", Institute of

Information Science and Electronics, University of Tsukuba, Japan. Department of CS, Georgia State University. University Plaza, Atlanta, GA 30303, USA.