IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Computer Networking

Name :- Dr. Khushbu Khandait
Designation :- Assistant Professor
College :- Ajeenkya D.Y.Patil University

Name :- 1.Vinut Maradur 2.Saurav Mehta 3.Vaibhav Kale
College :- Ajeenkya D.Y .Patil
University Pune , Maharashtra , India

Abstract-
Computer networks have become increasingly ubiquitous. In today's world, a computer network is much more than a collection of interconnected devices. Computer networks are a system of interconnected computers for the purpose of sharing digital information. The computer network enables to analyze, organize and disseminate the information that is essential to profitability. The rise of intranets and internets is the important aspect of computer networking. Intranets and internets are private business networks that are based on internet technology. The businesses are currently implementing intranets at a breakneck pace and for one reason only, an intranet enables a business to collect, manage and disseminate information more quickly and easily than ever before. Many businesses are implementing intranets simply to remain competitive; business that delay is likely to see their competition outdistance them. In this article we are presenting the basic concepts of networking.

Keywords- *Peer-to-peer; Client/Server ;Internetworks; Intra-networks; Communication medium; Internet Protocol; Open Systems Interconnection.*

I. INTRODUCTION

Networking supports communication between two or more programs running on physically distant machines. A computer network is a collection of computers, which are in some way connected such that they can exchange data between themselves and other computers on the network. A network is created when two or more computers are connected to share information and resources. A set of computers exchanging information by common conventions called protocols over communication media. A computer network is simply computers wired together in a way that lets them share data and/or devices such as hard drives, CD-ROMs, fax-modems, printers, etc[2].A computer network is an interconnected collection of autonomous computers where interconnected means that the computers can exchange information and autonomous means that no computer can start, stop or control another computer connected to the network. Fig 1 gives an example of a network in a school comprising of local area network or LAN connecting computers with each other, the internet, and various servers[4].

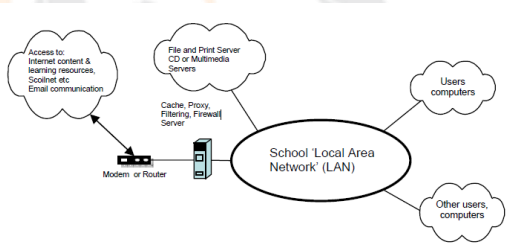

Fig 1: Representation of Network in a school.

II. TYPES OF NETWORK CONFIGURATION

Broadly speaking, there are two types of network configuration, peer-to-peer networks and client/server networks.

A. Peer-to-peer networks

Peer-to-peer networks are more commonly implemented where less than ten computers are involved and where strict security is not necessary. All computers have same status, hence the term „peer", and they communicate with each other on an equal footing. Files can be shared across the network and all the computers on the network can share devices such as printers or scanners, which are connected to any one computer. connected in a peer Fig 2 represents how the computers are -to-peer networks [4].

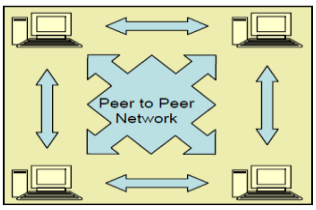

Fig 2: Peer to Peer Networking

B. Client/server networks

Client/server networks are more suitable for larger networks. A central computer, or „server", acts as the storage location for files and applications shared on the network. Usually the server is higher than an average performance computer. The server also controls the network access of the other computers which are referred to as the „client" computers. Only the network administrator will have access rights to the server while others cannot. Others can only use the client computers.

Fig 3 represents how the computers are connected in a client/server network [4].

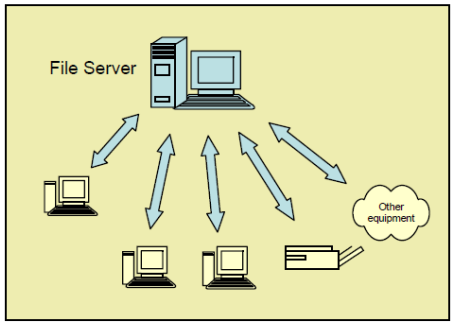

Fig 3: Client - Server Networking

III. COMPONENTS OF A NETWORK

A computer network comprises the following components:

- A minimum of at least two computers.
- Cables that connect the computers each other, although wireless communication is becoming more common.
- A network interface device on each computer (this is called a network interface card or NIC).
- A „switch" used to switch the data from one point to another. Hubs are outdated.
- Network operating system software [4].

IV. Types of network

The network can be divided into geographical areas and fall into these major categories.

- Local Area Network (LANs).
- Wide Area Network (WANs).
- Metropolitan Area Network (MANs).
- Wireless networks.

A. Local Area Network

A LAN is generally confined to a specific location, such as floor, building or some other small area. By being confined it is possible in most cases to use only one transmission medium (cabling). This technology is less expensive to implement than WAN because you are keeping all of your expenses to a small area, and generally you can obtain higher speed. They are widely used to connect personal computers and workstations in offices and factories to share the resources.Traditional LANs runs at a speed of 10 to 100 mbps have low delay and make very few errors. Never LANs may operate at higher speed up to 100 mbps.

1) Common Physical Topologies

Physical and logical topologies can take several forms. The most common and the most important for understanding the Ethernet and Token Ring topologies

are

- Bus topology.
- Ring topology.
- Star topology.
- Mesh topology.
- Cellular topology.

a) Bus topology

A bus physical topology is one in which all devices connect to a common shared cable. A physical bus topology network typically uses one long cable called a backbone computers (workstation and servers) are attached directly to the backbone using Terrestrial microwave-connectors. The backbone is terminated at

both ends to remove the signal from the wire after it has passed all devices. The bus topology is the first used topology to connect the computers in a network. This is the oldest form of topologies. This is a failure model.

Most bus topologies allow electric or electromagnetic signals to travel in both directions. A LAN with BUS

topology is represented in Fig 4.

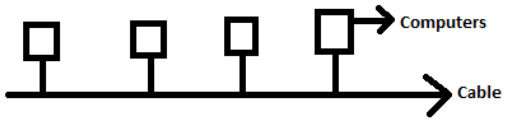

Fig: 4 LAN with BUS topology

b) Ring topology

Ring topologies are wired in a circle. Each node is connected to its neighbors or either side, passes around the ring in one direction only. Each device incorporates a receiver and a transmitter and serves as a repeater that passes the signal to the next device in the ring. Because the signal is regenerated at each device signal degeneration is low. After some period of time the RING topology came into existence. To avoid the disadvantages of BUS topology, the RING topology is invented. But this is also a failure model. Ring topologies are ideally suited for token passing access methods. The token gets passed around the ring, and only the node that holds the token can transmit data. Ring topologies are quite rare. A LAN with RING topology is represented in Fig 5.

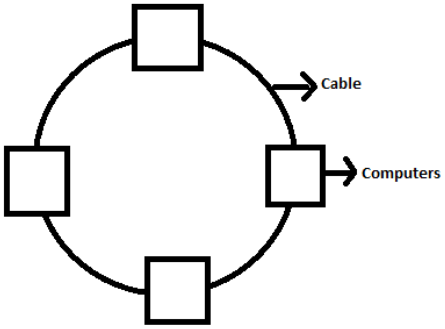

Fig: 5 LAN with RING topology

c) Star topology

Star topologies use a central device with drop cables extending in all directions. Each networked device is connected via a point-to-point link to the central device called a hub or multiport repeater or switch. Additionally, star topologies can be nested within other stars to form tree or hierarchical network topologies. In star topology, electrical or electromagnetic signals travel from the networked device, up its drop cable, to the switch, from there the signal is sent to other network. To avoid the disadvantages of BUS topology and RING topology, the STAR topology is invented. This is not a failure model. But it is a standard model and now-a-days this topology is commonly used everywhere. A LAN with STAR topology is represented in Fig 6.

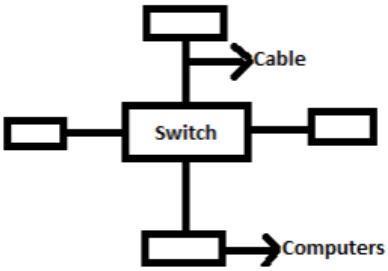

Fig: 6 LAN with STAR topology

d) Mesh topology

A mesh network has a point-to-point connection between every device in the network. Because each device requires an interface for every other device on the network, mesh topologies are not usually considered practical. However, mesh networks are extremely fault tolerant and each link provides guaranteed capacity.

e) Cellular topology

A cellular topology combines wireless point-topoint and multipoint strategies to divide a geographic area into cells. Each cell represents the portion of the total network area in which a specific connection operates. Devices within the cell communicate with a central station or switch. Switches are interconnected to route data across the network and to provide the complete network infrastructure. For example, devices may roam from cell to cell while maintaining connection to the network.

B. Wide Area Network

A wide area network spans a large geographical area, often a country or continent. It multiplies multiple connected LANs that can be separated by any geographical distance. In most WANs the network contains numerous cables or telephone lines, each one connection a pair of routers. If two routers that do not share a cable nevertheless and wish to communicate, they must do it indirectly. On personal computers we are using modem to communicate indirectly with other computer. WAN connecting two different networks is represented in Fig 7.

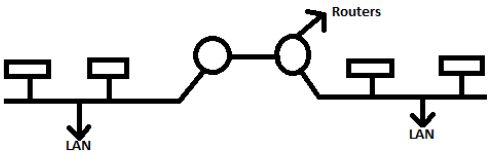

Fig: 7 WAN connecting two different networks

C. Metropolitan Area Network

Metropolitan Area Network is basically a bigger version of LAN and normally uses same technology. It might cover a group of nearby corporate offices or a city and might be either private or public. On the other hand, MAN is network running throughout a metropolitan area such as a backbone for a phone service carrier. A MAN just has one or two cables and does not contain switching elements.

D. Wireless Networks

Mobile computers such as notebook computers, laptops are the fastest growing segment of computer industry. Users want to connect this machine to their office LANs to see the data when they are out from the office, since the wired connection is not possible we have to use wireless networks. For e.g. on aircraft single router will maintain a radio link with some other router on ground, changing routers as it flies along this configuration is just a traditional LAN, except that its connection to the outside world happens to be a radio link instead of a wired line.

V. COMMUNICATION LINKS

Various types and forms of communication medium are

- Fiber-optic cable.
- Twisted-pair copper wire.
- Coaxial cable.
- Wireless local-area links. (e.g. 802.11, Bluetooth)
- Satellite channel [3].

VI. INTERNET PROTOCOL (IP)

To solve the scaling problem with Ethernet, and to allow support for other types of LANs and point-topoint links as well, the Internet Protocol was developed. To support universal connectivity, IP provides a global mechanism for addressing and routing, so that packets can actually be delivered from any host to any other host. IP addresses (for

the most common version 4, which we denote IPv4) are 4 bytes (32 bits), [6] and are part of the IP header that generally follows the Ethernet header. The Ethernet header only stays with a packet for one hop; the IP header stays with the packet for its entire journey across the Internet. An essential feature of IPv4 addresses is that they can be divided into a "network" part and a "host" part [5]. There are different types of classes in IPv4 and their ranges are shown in Table 1.

Table: 1 Range and types of classes

Class	Address Range
Class A	0 to 126
Class B	128 to 191
Class C	192 to 223
Class D	224 to 239
Class E	240 to 254

VII.OPENSYSTEMSINTERCONNECTION(OSI) MODEL

In 1977 the International Organization for Standardization, or ISO, founded the Open Systems Interconnection model, or OSI, a process for creation of new network standards. OSI represented an attempt at the creation of networking standards independent of any individual government. The OSI model is today perhaps best known for its seven-layer networking model. Those seven layers of the OSI model and their purpose are stated in Table 2. OSI has its own version of IP and TCP. The IP equivalent is CLNP, the Connection Less Network Protocol, although OSI also defines a connection oriented protocol CMNS. The TCP equivalent is TP4.

CONCLUSION

Computer communication, it seems, will become a much more useful networking tool when large numbers of people with similar interests acquire access to the technology. Though it can expedite the formation of new interpersonal networks by overcoming the space and time barriers faced by traditional networking techniques, it still requires a great deal of concentrated effort and resources to get the people to use it. This problem should become increasingly minimized over the coming years as the technological innovations become more diffused throughout society [8].

Information Domain

Abstract

Most abstract models of cooperative work concentrate on the procedural and structural aspects of group working. However, one of the fundamental processes that occurs when people work together is that of information sharing. This paper suggests that a complete model of cooperative work would benefit from explicitly incorporating the concept of information sharing. It is proposed that this can be achieved by including information domains in such a model .Two projects that have addressed this issue to a limited extent are outlined and compared. Finally, four areas of consideration are identified and discussed, and areas for further research are highlighted.

Introduction

Over the last few years there has been a considerable amount of research devoted to the subject of computer supported co-operative work (CSCW). Many areas have been addressed within this field, ranging from the development of underlying technologies to support CSCW, through studies of group working in general, to the proposal of abstract frameworks modelling group communication using computers. This paper discusses an issue that has been touched on by many different researchers working in widely varying areas, yet has not been fully explored in its own right. A key consideration for any approach to CSCW is that of information, in particular, the sharing of information. Underlying support for this has been developed (e.g. [11]), and there is much ongoing research into more efficient ways of managing the storage and access of information . Over large computer networks. However, a coherent model of information sharing within an organisation has yet to be developed. This paper will demonstrate that, not only is a model of information sharing necessary, but that such a model can be integrated with mode is of procedural and structural aspects of group working in order to develop a complete and coherent description of CSCW. It will also identify and discuss some of the issues involved in modelling information sharing. The concept of an information domain is introduced to facilitate the modelling of information sharing. An information domain is a grouping of people and/or roles, information objects, and other resources. This grouping represents a working group in real life, that is, it brings together people, information, and necessary tools and services so that a goal or set of goals can be achieved.

The information domain represents the collection of functions for gathering data from various domains, most significantly from the control domain, and transforming, persisting, and modelling or analyzing those data to acquire high-level intelligence about the overall system.

The data collection and analysis functions in this domain are complementary to those implemented in the control domain. In the control domain, these functions participate directly in the immediate control of the physical systems whereas in the information domain they are for aiding decision making, optimization of system-wide operations

and improving the system models over the long term. Components implementing these functions may or may not be co-located with their counterparts in the control domain. They may be deployed in building closets, in factory control rooms, in corporate data centers, or in the cloud as aservice.

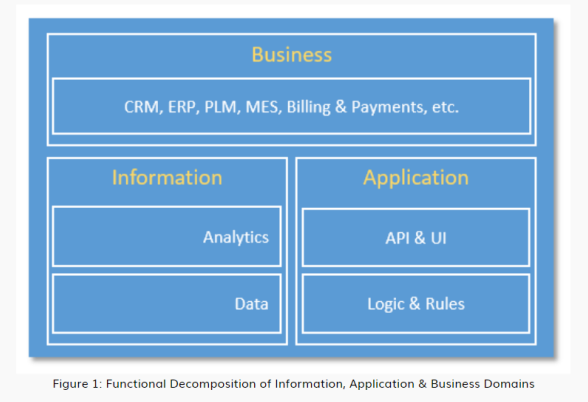

Figure 1: Functional Decomposition of Information, Application & Business Domains

Data

Data consists of functions for:

- ingesting sensor and operation state data from all domains,
- quality-of-data processing (data cleansing, filtering, de-duplication, etc.),
- syntactical transformation (e.g., format and value normalization), semantic transformation (semantic assignment, context injection and other data augmentation processing based on metadata (e.g. provisioning data from the Operations Domain) and other collaborating data set,
- data persistence and storage (e.g. for batch analysis) and
- data distribution (e.g. for streaming analytic processing).
- These functions can be used in online streaming mode in which the data are processed as they are received to enable quasi-real-time analytics in support of orchestration of the activities of the assets in the control domain. They may be used in offline batch mode (e.g. seismic sensor data collected and accumulated in an offshore oil platform that does not have high-bandwidth connectivity to the onshore data center).

  Data governance functions may be included for data security, data access control and data rights management, as well as conventional data management functions related to data resilience (replication in storage, snapshotting and restore, backup & recovery, and so on).

Data Analytics

Analytics encapsulates a set of functions for data modelling, analytics and other advanced data processing, such as rule engineers .The analytic functions may be done in online/streaming or offline/batch modes. In the streaming mode, events and alerts may be generated and fed into functions in the application domains. In the batch mode, the outcome of analysis may be provided to the business domain for planning or persisted as information for other applications. The data volume at the system level in most IOT systems will eventually exceed a threshold at which the traditional analytic toolsets and approaches may no longer scale in meeting the requirement in performance. “Big Data” storage and analytic platforms may be considered for implementing these functions.

Information domains for information sharing

Many abstract models of group working have been put forward in recent years. These have
been formulated using several different approaches, which can be categorised in many ways . Group communication has been modelled from the point of view of the data involved , the agents involved the existing communication structure and the processes involved both at the level of individual turns in an activity and at the level of describing the activity itself . All the above models of group working describe its procedural aspects. Most of them also include some concept of the structural aspects 'of communication. However, a striking omission from all these models is the notion of information sharing.
When a group of people forms with the intention of working together to achieve a particular goal or series of goals, some sort of context is implicitly or explicitly created within which this group will work. Members of the group will use this context to share information and tools pertinent to the tasks involved in attaining the goal(s). Goodman and Abel call this context a project space. Their work involved looking at groups, focusing on patterns of communication and realisation of project spaces. Groups that they looked at were working groups within a department, rather than departments within an organisation, but it seems likely that larger groups with less well-defined goals will also use contexts similar to project spaces to share resources. It seems, then, that information domains are generally used in some form by groups of people working together. If communication within these groups is to be supported by a computer system based on a model of processes involved in group working, IDs will still be created and used to share information objects and resources. Therefore, it makes sense to provide support for this by including the concept of IDs in the particular model used, and thus providing an integrated support service.

Information domains for object naming

In addition to the advantages of using explicitly defined information domains to support information sharing, an ID may be integrated with an object naming scheme. Object naming is usually considered to be entirely local (the meaning of a name is private to individuals), or entirely global (a name means the same to all users). Most systems using a global naming scheme allow individuals to

give private aliases to objects, but in a group working environment this does not give enough flexibility. Sollins and Clark [21] propose a naming scheme that allows self-defining groups to jointly create and use names. The scheme relies on arbitrarily defined contexts, which are associations between groups of people and sets of names for objects. A name can be used to access the
object it refers to, and it acts as a placeholder for the object. The attributes of cOl ltexts
could easily be associated with IDs within a model of group working, as it is likely that
groups defined by the two methods will overlap to a significant extent . Kreifelts and Seuffert [14] describe the addressing scheme used in the DOMINO office procedure system. This relies on the definition of organisational units, which are groups of people within an office. Each organisational unit may contain other organisational units, or a set of projects, which are groups of people with specific goals. People may be referred to by their position in one of these units. A logical progression from this definition is to allow the inclusion of information objects in these groups, thus incorporating the information sharing aspects of group working.
Standard naming schemes such as that provided by the joint IS 0 jCCITT international directory standard ISO IS 9594, CCITT X.500 [4J can also be usefully integrated with information domains. The directory is represented as a tree, with general denominators such as countries at the top, and progressing downward through organisations and departments to names of people and objects. The global (distinguished) name of an entry is given by the entire path through the tree to its vertex, and its local(relative distinguished) name is given by the lowest
of the identifiers, thus providing a name for the object at the level of a group. Organisations, departments, and groups can all be mapped to IDs.

Information domains for defining groups

The final reason for including information domains in a model of group working is to allow the definition of limits for groups. This can be useful in a number of ways, for example:
easy identification of members of the group becomes possible,
• restricting access to information is made easier,
• tools and resources needed for task performance may be made available to group members.
There are two important consequences of explicitly defining groups using information domains. The most obvious of these is the possibility of constraining the scope of operations such as searching, modifying, and reading information objects. This is becoming increasingly important as the size and complexity of computer systems and networks increases. For instance, it would not be very efficient to search all the documents in a large organisation for one particular document. The search could easily be constrained by specifying which group is likely to have possession of the document, and therefore, which information domain it can be found in.
The other consequence of defining groups using information domains is that it becomes possible to associate activity management specifications with explicit groups·. Benford has identified the need for these *local management policies*, which further specify the performance of tasks within specific local environments. These environments could easily be mapped onto groups as defined by information domains.

Creation and maintenance of information domains

The main purpose of information domains is to facilitate as far as possible the sharing of information. Thus, it must be easy to create and maintain lDs, and this should not interfere unduly with performance of activities in general. Any future development of IDs needs to consider this aspect when specifying their structure. For example, guidelines on the possibIe contents of an information domain, and their specification .

The process of creating an information domain is likely to follow an identifiable pattern, for example:
1. Create an ID and give it a name
2. Specify the contents of the ID and its maintainer
3. Notify the contents that they belong to the ID
4. Notify other entities of the ID's existence
5. Specify any management policies' associated with the ID
This pattern will depend on the particular model of IDs that is de-"eloped, but once that has been specified, the tasks associated with creation will become apparent. The mechanisms of the procedural part of the model of group communication could then be used to define the activity of ID creation in order to provide additional support for the end-user. When considering the maintenance of lDs, the degree that the ID and its contents are permitted to change will be decided upon. There are several possibilities here, ranging from no permitted change, through change of contents only, to change of both contents and properties of the ID. It *is* likely that any group will need to change its contents; to add a new member, or include a new information object. It is less likely that the basic properties of the group will change, but it is still possible (e.g. the work of a group suddenly becoming secret), and
so that may also be considered. The other consideration concerning ID maintenance is the degree of automation of this maintenance that is possible. The solution at the moment would be to define a role of administrator that has to be instantiated for every information domain, and provide a set of guidelines for the person playing the foie to follow. However, there is a growing interest in the specification of activity management policies , and it is possible that this work could be applied
to the automation alid support of ID maintenance. Also, the maintenance of an ID could be considered to be an activity in itself, and. therefore the procedural aspects of the model could again be used.

Acceptance of the information domain concept

For efficient information sharing, end-users need to understand and accept the concept of an information domain. This can be achieved by defining IDs so that they reflect the formal and informal group structure that exists in real life. There are three implications of adopting such a structure for IDs:

• The structure of groups within an organisation is very dynamic; groups will often be formed, broken up, or changed in some way.
• Groups often overlap with, or 'exist entirely within, other groups.
• There are often different types of groups within an organisation. '

'All these implications should be considered when modelling information domains, in order to allow the end-users to assimilate the concept and use it effectively for information sharing.

The dynamic nature of groups indicates that the creation and maintenance of lDs (dealt with in the previous section) should be as flexible as possible, and should not interfere with normal group working. In addition, the increasingly distributed nature of computer installations will make it very difficult for a central entity to keep track of changes in group structure, although it would be possible. It would be more efficient to define IDs that are relatively autonomous and self-regulating.

The naming policy that is used could be affected by overlapping IDs, if it is sufficiently complex. If an information object exists in two overlapping groups with a different name in each, difficulties could arise. Another problem that needs to be addressed when considering overlapping IDs is that of management policies. If two groups with different policies and controls overlap, a conflict may arise. Further study is needed here, both into what happens in real life, and into possible ways of modelling these processes. Organisations may contain many different types of groups that differ in many ways. For example, some groups may be more or less permanent (e.g. departments), whereas others may be formed solely for one short-term activity (e.g. entities involved in organising a trip) some groups may be secret, others may be open and soon. A sensible categorisation of these groups is needed, from which it should be possible to see whether different types of ID need to be defined, or whether the various types of groups can be reflected by differing attributes of the same ID type.

Internal structure of information domains

The general issues of creation and maintenance of IDs, and the users acceptance of the concept of IDs, must be considered when defining information domains. The process of creating all information domain is likely to follow a particular pattern, as discussed earlier, and this may be partly identified from the· contents and attributes of the ID. It therefore follows that these properties should be specified in a model of information domains, even if some are specified as optional. Examples ohhe types of properties that may be specified are:

• Name - an identifier by which the ID is referred to.
• Description -·a textual description of the purpose of the ID.
• People/Roles - human entities included in the ID.
• Information objects documents etc. included in the ID.
• Storage information - description of the organisation of information objects.
• Resources - tools and services available within the ID.
• System agents - automated entities that exist in the ID.
• Management information .

In addition to specifying which properties may be used, some guidelines on their use may be defined. For example, instead of just stating that a set of resources may be include the format of the expression to include them may be specified as follows:

resource-component = <name> <description> <access-procedure>

These guidelines may be applied equally well to the processes of creation and maintenance of IDs. It would also be possible to specify constraints on the number or type of a particular entity that should be included a type of ID.. For example, it could be specified that a department has between 3 and 30 people, exactly one of which will play the roles of department head. The internal structure of IDs should reflect as far as possible the internal structure of real-life groups. That is, it will include all the entities that may be associated with a group in reality, and the guidelines and constraints on the specification of the contents of an environment should be sensihleand easily understood. In particular, if different types of information. domains ate required and defined, their specified contents will reflect the IDs' purposes.

Properties of information domain boundaries

Creation, maintenance, and acceptance of IDs also need to be considered when defining the properties of ID boundaries. Any properties that may have to be refined at creation time, or during the lifetime of the ID, should be carefully specified, along with guidelines for their refinement. Also, the way ID boundaries are specified should allow groups to be formed in the same way that they are formed in reality. There are two major properties that ID boundaries may possess that need to be considered:

Transparency - controls the visibility of the contents from the outside.

There are four degrees of transparency and access that an ID boundary may possess. First, it may be completely opaque; so that no entities outside can see or· access its contents. Second, it may be completely transparent, so that all its contents are visible to the outside but not accessible. Third, it may be transparent and all contents may be accessible. These three

possibilities present no problem. The fourth possibility is that some of the contents are visible to the outside, and others are invisible (some or all of the visible contents may be accessible). In this case, some mechanism for achieving this must be provided. One possibility is to make the ID responsible of taking
requests to view or access contents, and referring to lists of visible and accessible contents when deciding which to display or allow access to. Whatever mechanism is chosen, it ought to be transparent to the end-user.

Conclusion

The previous sections have described the concept of information domains, outlining reasons for their incorporation into models of group working, describing past work on the subject, and identifying important issues that must be considered when modelling information domains.
Although low-level support for information sharing has been investigated to some extent, most models of cooperative work developed so far do not take into account information sharing aspects of group working, but concentrate on procedural and structural aspects.
This paper has argued that there are three main reasons for including information sharing aspects in general models of group working. The first, and most important, of these is to facilitate and support efficient information sharing in a CSCW environment. Secondly, the integration of an object naming scheme that does not rely totally on global naming is provided
for. Finally, the clear definition of working groups and the interaction of these groups becomes possible. It is suggested that the need for the inclusion of information sharing aspects in group communication models could be met by incorporating the notion of an information domain. It has become apparent from looking at existing treatments of IDs that there are many issues to be considered and researched before a coherent model of information domains is developed. It seems likely that some of these issues may be resolved by investigating teal-life group interactions, and modelling how information is shared and groups are formed in reality. In addition, extra support for the end-user should be provided so that the mechanisms for creating, maintaining, and using information domains do not inhibit the efficient performance of organisational processes. The integration of procedural, structural, and information sharing aspects of modelling cooperative work should be relatively easy. The use of information domains in itself helps to integrate the latter two aspects, by providing a basic structure which to build more detailed structural distinctions. Procedural definitions within the model will be used to define ID creation and maintenance processes, and IDs, once they have been created, can be used to contain all the entities involved in a particular activity.

There is much scope for further study of the information domain concept, and of information sharing in general. The three reasons for including IDs outlined in section 2 by no means exhaust the possible uses of information domains; further research would doubtless reveal more possibilities. There is a need for the investigation of the interaction between groups, and the different types of groups, that exist in real life. In addition to these problems, the issues highlighted in section 4 also need further consideration. The whole concept of an information domain is relatively new, and there are many problems. to be resolved. It seems clear that models of procedural and structural aspects of group communication are not enough to facilitate true computer supported cooperative work. It has been recognised that, at the most basic level, group working involves groups' of people performing tasks, according to certain patterns. However, in order to do this, these people need information, and they need to be able to share that information.

Transportation Domain

Abstract:

Intelligent Transportation Systems (ITS) are emerging field characterized by complex data model, dynamics and strict time requirements. Ensuring cybersecurity in ITS is a complex task on which the safety and efficiency of transportation depends. The imposition of standards for a comprehensive architecture, as well as specific security standards, is one of the key steps in the evolution of ITS. The article examines the general outlines of the ITS architecture and security issues. The main focus of security approaches is: configuration and initialization of the devices during manufacturing at perception layer; anonymous authentication of nodes in VANET at network layer; defense of fog-based structures at support layer and description and standardization of the complex model of data and metadata and defense of systems, based on AI at application layer. The article oversees some conventional methods as network segmentation and cryptography that should be adapted in order to be applied in ITS cybersecurity. The focus is on innovative approaches that have recently been trying to find their place in ITS security strategies. These approaches includes blockchain, bloom filter, fog computing, artificial intelligence, game theory and ontologies. In conclusion, a correlation is made between the commented methods, the problems they solve and the architectural layers in which they are applied.

Keywords**:** ITS; IoT; VANET; cybersecurity

Introduction

Internet of things (IoT) is a consequence of converging of several technologies like: real-time

analytics, machine learning, embedded systems, wireless networks, control systems, home and building automation. From the consumer point of view, IoT is a synonymous to products pertaining to the concept of the intelligent home, intelligent healthcare, intelligent city and so forth. Many of these areas have similar characteristics and face similar challenges. Borrowing technologies between IoT sub-areas is common but needs to be considered well and explored in practice. Despite the similarities, even within the same area the requirements for communication range and bit rate, real-time operation, reliability and security vary. As sub-area of the smart city Intelligent Transportation Systems (ITS) are characterized by many of the features of IoT. Their distinctive features are: strict time requirements, dynamics and large volumes of data. One of the main characteristic property of the ITS is the high demand of cybersecurity. ITS applications can be classified as: transport safety, road traffic efficiency and infotainment. Road safety applications have very high cybersecurity requirements combined with hard real time constrains. Although road traffic efficiency and infotainment applications are not directly related to the physical safety of road users, cybersecurity requirements remain high, as a breach in any of them can reflect on the efficiency of the whole ITS. For example, overloading the communication channel for infotainment application purposes may interfere with the normal operation of security application, which may be critical.

Vehicular ad-hoc networks (VANET) are a key component of all modern developments for ITS. Nodes (vehicles) in VANET exchange short messages, called beacons, during certain period. The beacons contain important information about vehicles and the environment, for example, direction, acceleration, speed, road conditions, weather conditions and so forth. Connecting vehicles in wireless one hop communication poses many tasks such as authentication of newly joined vehicles, the need to protect the identity of the user, interruptions, providing multi hop communication, high heterogeneity (depending on whether the cars are congested in a big city or in a suburban area). Much of the research on ITS cybersecurity focuses on network security.

ITS Cyberattacks :

The heterogeneity of ITS complicates the task of classifying and identifying cyberattacks. This section lists ITS specific attacks, which will later be associated with the architectural layers:

VANET Man-in-the-Middle Attack

The man-in-the-middle attack is a classic type of cyberattack, that the attacking party intercepts messages between the two communicating parties and forwards modified content. In case of man-in-the-middle attack on the physical and data link level in VANET, the attacking party take into account the fact that the nodes have a certain range. They either have to attenuate the signal or they have to modify the location information in case they take advantage of a situation where the attacked nodes are out of range but the attacking party is in the range of both nodes. Example of man-in-the middle VANET attack: the attacking party interferes in the communication between two or more vehicles and changes their location information. This can disrupt the proper functioning of road safety or efficient traffic applications.

Routing Attacks

The physical and the data link level of VANET define one-hop communication. Multi-hop communication is provided by routing protocols. Routing attacks are cases in which there is a breach in the routing protocols of VANET and a malicious node prevents the data from reaching their final destination. Black hole attack is an example of a routing attack in which, malicious node silently drops all the packets, that are supposed to be re-transmitted. Gray hole attack is another sub-type of routing attack in which dropping is performed only on selective packets.

Timing Attacks

Timing attacks cause a communication delay and thus disrupts the operation of applications that have real-time requirements. For example, in a cooperative adaptive cruise control system an emergency message is sent to the neighboring vehicle in order to prevent collision. If the attacking party manages to cause a delay (for instance by overloading the network traffic), despite the correct receipt of the data, the reaction in the braking system will delay and the collision will not be prevented.

Spoofing

In case of spoofing attack the attacking party broadcast corrupt data in order to cause invalid reaction in the system. Example: The attacking party is sending bogus GPS coordinates and thus disrupting the operation of the navigation system.

Denial-of-Service Attacks (DoS)

DoS is a classic cyberattack that affects the availability of system components. In ITS it is especially dangerous in case some safety critical

feature is concerned. Sybil is typical VANET DoS attack in which a malicious vehicle impersonates as multiple identities and injects false broadcast messages into the network. Thus disrupts the normal exchange of information.

Internal Vehicle Network Attack

Due to the fact that most internal vehicle networks are designed at a time when cars are not connected, they are vulnerable to attacks. For example, the attacker can easy gains access to the internal network, based on CAN (Controller Area Network) protocol and thus manage to control airbag control system.

Identity Attack

Identity privacy ITS may refers to the privacy of a driver, passenger, pedestrian and so forth. The attacking party may try to extract information about personal data, location, actions, habits. An example of an identity attack is a case in which the attacking party manages to obtain information on how nicknames are assigned in VANET and thus track the location of a vehicle.

Eavesdropping

Eavesdropping is a classic passive attack in which the attacking party does not disrupt the communication process but manages to gain unauthorized access to information. Example: The malicious party may eavesdrop on the communication between the vehicle and the road infrastructure during the payment of the toll and thus gain access to the user's bank account details.

Attack against Fog

Due to their physical characteristics (usually physically accessible) and limited resources in comparison to the Cloud, ITS's Fog components are difficult to protect and can be subject to various types of attacks. Example: Fog node summarizes and purifies data from sound and vibration sensors. By altering the aggregated information, the malicious party directly affects the data analysis algorithm for planning the organization of the road traffic.

AI Attacks

The attacks against AI could be related to data manipulation (Data poisoning attack), Environmental Perturbations or Policy manipulation. Example: In order to mislead the machine learning algorithm, the attacking party may select and send data so as to cause false trends in the model.

ITS Architecture and Security Challenges

The ITS can be seen as a sub-type of IoT and so it can be developed using similar approaches and architectures. The Figure 1 depicts the architecture contours of most IoT developments. It could also be applied in ITS.

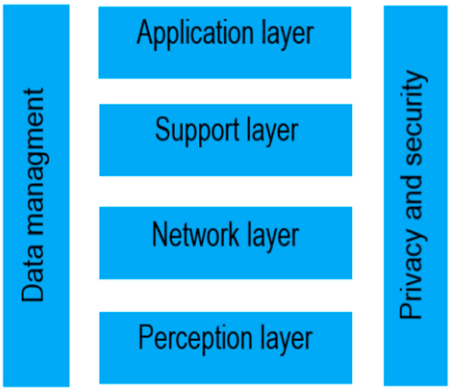

Figure 1. Internet of things (IoT) architecture outlines.

The presented architecture consists of four layers responsible for different functions of IoT.
Applying this Outline in ITS gives each layer a more specific functions.

Conventional Methods in ITS Cybersecurity

Although ITS are relatively new, many of the technologies they integrate have been tested in practice and the experience gained can be reused. In terms of security, some of the classic approaches will certainly play a key role. The effective approaches of defending support layer are: strong authentication, encrypted communication, key management, regular auditing and private network and secure routine .

Cryptographic methods are the heart of cybersecurity. The application of cryptographic techniques in the automotive industry has a history since 90s. Traditional algorithm and encryption standards are not completely suitable for ITS as they cannot meet the requirements of high throughput performance, low latency and reliability. Lightweight encryption has become a basic requirement in ITS.

Network segmentation is another classic approach that improves both network security and efficiency. When talking about ITS network segmentation, it should be taken into account that some of the nodes are mobile, dynamically joining and with anonymity requirements. In VANET, the separation of clusters from communicating cars would play an important role, thus building hierarchy in the network. Depending on the goals and the situation, different metrics can be taken into account—the behavioral characteristic, based

on historical data, the resources, the location and so forth.

Innovative Approaches in ITS Cybersecurity

The introduction of technologies that were not originally designed to serve time-critical areas, as well as introduction of technologies from areas where cybersecurity is not directly related to users' physical security, leads to an increase in the vulnerability to cyberattacks in ITS. Borrowing technologies between different sub-areas in IoT is quite natural. In this section some innovative technologies that have found application in ITS or have found application in similar areas and their application in ITS is yet to be experimented with are presented. Given the multi-faceted nature of ITS, approaches to achieving cybersecurity objectives are multidimensional. Methods discussed in the Section 6 relate to the application layer and are holistic in nature, while this section discusses methods that have a local impact—in the network and perception layer. Blockchain, anonymous authentication in Fog and bloom filter are applicable in resource reduction in anonymous authentication of dynamic nodes in VANET. Security-by-contract and sensor fusion are applied in the sensor layer. Although data fusion can take place in any of the layers in the system, the sensor fusion approach is related to the perception layer, as the closer to the source the information is processed the less security risks exist.

Blockchain

Blockchain is an extremely dynamic technology in recent times. With regard to ITS, one of its main applications is in anonymous authentication solutions in VANET. The use of distributed storage can be very suitable for storing data of the legitimacy of nodes. The nodes decide whether to admit a new participant in the communication based on its reputation. In this way, malicious nodes are discouraged. Another option for applying a blockchain is upper architecture layers as a secure data warehouse. Although some of the described examples present MANET networks, the simulation results can be considered to be applicable to VANET as a subtype of MANET.

Anonymous Authentication in Fog

As Fog nodes provide precious opportunities to protect the privacy of the consumers before personal sensitive data leave the edge. Fog technology is one of the solutions to the problem of anonymous authentication in VANET.

Bloom Filter

Bloom filter is another solution to the issue of reducing resources when using changing aliases.

Security by Contract

Security by contract paradigm is based on a description of the relevant features of the application and the relevant interactions with its host platform. This approach is a possible solution to many of the security tasks in the sensor layer, as it is also applicable to devices that are put into operation.

Sensor Fusion

Sensor fusion can offset incorrect information from corrupting computations and reducing data

ambiguity. A great advantage of this technology is that it allows the use of inexpensive sensors and thus significantly reduces the final cost of the products without affecting the measurement result.

Sensor fusion is already applied in practice in many modern automobiles.

An Intelligent Security in IoT

Due to the complexity of ITS an intelligent and proactive defense approach is a necessity. The methods described in this section relate to the holistic approach of ITS cybersecurity and have been successfully applied in security systems in other areas. In relation to ITS, they are mentioned on many sources as methods that will outline the overall appearance of ITS in the future but still the experimental results of their application in ITS are few. This is largely due to the fact that the development of the whole system is not mature enough. This section discusses examples of the application of artificial intelligence, machine learning, ontologies and game theory in security systems.

Artificial Intelligence

With the advent of IoT, AI is increasingly used in Intrusion Detection Systems (IDS), due to the increased risk to security and complexity of tasks. AI will definitely find a place in future ITS cybersecurity, due to the need for adaptive solutions to the rapidly changing system and the need for a holistic approach.

Machine Learning

Machine learning (ML) is the subset of AI that is most widely used in cybersecurity systems. Its weakness is that it is vulnerable in the training phase, so the training data set must be carefully selected. If a noise is inserted, the whole system can be compromised (Envision Attacks, Poisoning Attacks). It is necessary to create a strong classifier through proactive approaches. Due to this disadvantage, ML techniques are often used as an auxiliary mechanism.

6.3. Ontology

Ontology is a promising tool to address heterogeneous issues, especially for unstructured data. The application of ontology to the IoT security domain is an emerging area.

Game Theory

Game theory is a powerful mathematical tool that has been successfully applied in the fields of cybersecurity and privacy.

References:

1.Han, M.; Liu, S.; Ma, S.; Wan, A. Anonymous-authentication scheme based on fog computing for VANET. PLoS ONE. [Cross Ref] [PubMed]

2. Jin, H.; Para dimitratos, P. Proactive certificate validation for VANETs. In Proceedings of the IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA,.

3.IEEE. IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Application sand Management Messages; Revision of IEEE Std; IEEE: Pictasaway, pp. 1–240.

4.Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. J. Cloud Computer. Adv. Syst.. [Cross Ref]

5.Mir, Z.H.; Filali, F. LTE and IEEE 802.11p for vehicular networking: A performance evaluation. J. Wirel.Commun. Network . [Cross Ref]

6.Hahn, D.A.; Munir, A.; Behzadan, V. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. IEEE Intel. Transp. Syst. [Cross Ref]

7.Huawei Technologies Co., Ltd. 5G Security Architecture White Paper; Huawei Technologies Co., Ltd.: Shenzhen, China.

8. Deshpande, V.; Das, T.; Badis, H.; George, L. SEBS: A Secure Element and Blockchain Stratagem for Securing IoT. In Proceedings of the 2019 Global Information Infrastructure and Networking Symposium (GIIS), Paris ,France ; pp. 1–7. [Cross Ref]

9.Rahimi, N.; Maynor, J.; Gupta, B. Adversarial Machine Learning: Difficulties in Applying Machine Learning to Existing Cybersecurity Systems. EPiC Series Computer. 69, 40–47. [Cross Ref]

10.Cherita L. Corbett, Raheem A. Beyah, John A. Copeland, Using Active Scanning to Identify Wireless NICs, in: Proceedings of the 7th IEEE Workshop on Information Assurance, U.S. Military Academy, West Point, NY, 21-23 June 2006.

11.Pranab Kumar Chakravarty, Computer Networking Technologies and Application to IT Enabled Services.

12.Antonio Carzaniga, Basic concepts in Computer Networking, September 19, 2014.

13.Teodora Bakardjieva, Introduction to Computer Networking.

14.Peter L. Dordal, An Introduction to Computer Networks, Release 1.8.07, June 16, 2015.

15.Bob Dickerson, Computer Networks, January 2005.

16.Russell Anthony Tantillo, Network Security through Open Source Intrusion Detection Systems, May 2012.

17.http://web.net/~robrien/papers/mpconclusion.html

18.http://www.computerhope.com/jargon/i/ip.html

19.L. Aiello, D. Nordi, and M. PantL Modelling the office structure: A first step towards the office expert system.

20.E. Auramaki, E. Lehtinen, and K. Lyytinen. A speech-act-based modelling approach.

21.S.D. Benford.. Requirements of activity management. In ProceeClings of the 1st European Conference on CSCW, 1989.

22.S.D. Benford. Components of OSI: 'the eSI directory service. In Connexions: the interoperability report, pages 2-9, Summer 1989.

23.J. Bowers, J. Churcher, andT. Roberts. Structuring computer-mediated communication in COSMOS. EUTECO '88 - Research into networks and distributed applications, pages 195-210, 1988.

24.G. Bracchi and B. Pernici. The design requirements of office systems. A CM Transactions on Office Information Systems, 2(2):151-170, 1984.

25.K. Crowston, T.W. Malone, and F. Lin. Cognitive science and organisational design: A case study of computer conferencing. In Pl'oceedings of CSCW '86, pages 43-61, 1986.

26.F. De Cindio, G. De Michelis, and C. Simone. Groups in a'language/action perspective. Cosmos Information Exchange Network, pages 5-18, 1988.

27.F. Flares, M. GraNes, B.IIa.rtfield, a.nd T. Willograd. Computer syst.ems a.nd the design or organisational iIiteraction. .A CM Tmnsactio1/.s on Office Information Systems, 6(2):1.53"172, 1988.

28.G. Goodman and M. Abel. Collaboration research in SCL. In Proceedings of CSCW "86, pages 246-251, 1986.