Networking and Security

CRN: 50251

Network Design and Related Aspects

Roll Number

@00677611

Table of Contents

Introduction

In this report, split into 2 sections; the former of, I discuss the function, purpose, benefits, drawbacks and future of Intelligent Transportation Systems including some first hand experience. I chose to write about Intelligent Transportation Systems as I have some background in automation, IoT and optimisation of interaction at home and find it personally interesting.

In the latter section, I go through the process of subnetting an example network, giving justifications in the form of sentences and tables. Later comparing default and explicit routes, giving examples using Cisco's IOS command line, and comparing static and dynamic routes. In the final task, discussion of TCP and UDP, describing their function, application, advantages and disadvantages. Finally, I will explain the OSI model and its purpose, and also briefly it's shortcomings.

Section 1 – Show and Tell

Intelligent Transportation Systems: Reworking Movement

Introduction

For the past 4 years, I have found enjoyment in deploying services using Docker for lifestyle improvement. One group of services involves platforms for managing IoT devices and connecting systems together (ex. Grafana, InfluxDB, HomeAssistant, MQTT, Frigate). The aspect of data collection to form an output that directly benefits efficiency and convenience was interesting to me and useful to this day. However, the process of learning how to create interconnected networks of IoT devices was not without it's speedbumps – troubleshooting firewall rules across VLANs, ensuring proprietary IoT devices can't call home and integrating them with systems they were never built for. This experience directly ties in with the concept of ITS; just as my IoT devices interconnect with each other to elevate my home, ITS use connected technologies to optimise routes, improve safety and adapt traffic patterns. Imagining how home automation and optimisation can be applied to entire cities' transportation networks, if I can save 2 minutes every day by collecting the data from a camera myself using Frigate, what is to say millions living in an intelligent city can't have time saved by implementation of ITS.

What are Intelligent Transportation Systems?

An Intelligent Transportation system is part of IoT (Internet of Things), allowing devices to be interconnected to maximise efficiency and minimise congestion. An ITS allows for V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) communication (Chipilska, 2024); a car could communicate with another car to warn of an incident on the road; a car can communicate with a person's smart home to turn on the heating 15 minutes from arrival. (RantCell. 2024)

ITS' concept in the UK originated in the 60s with investment in transport infrastructure, and was implemented in the 80s and 90s in the form of Advanced Traffic Management Systems with the aim to reduce congestion. Using cameras, sensors and software to adapt traffic, this provided real-time information and allowed easier detection of incidents. In the 2000s, the widespread introduction of GPS allowed for elevated traffic information directly to drivers, helping with journey planning; the UK government also introduced Intelligent Transport Management Systems to further reduce congestion and optimise the transport network. This brings us to the current day, where our government has recently introduced initiatives to develop and deploy Connected (and) Autonomous Vehicles (CAV). ITS in our decade has become an essential part of our efficiency of mobility, safety and sustainability of the transportation network. (WJ Group, 2023)

Henceforth, ITS implements many technologies / concepts to allow for it's improvements to the transport network. (Quan, 2023)

- 5G has been the one of the biggest steps in allowing the interconnection of V2X (Vehicles-to-Everything) in recent years, maximising network traffic throughput and minimising latency on cellular networks, allowing for a previously unrivaled flow of information.
- IoT while not being a recent concept, is integral to ITS, providing small internet-connected devices with specific purpose. Namely cameras, environmental sensors, LIDAR, GPS trackers, telematics, etc. These devices while not entirely useful singularly, when interconnected allow for a great amount of data to be adapted or mined for an output. (Andriy. 2024)
- AI can be integrated with IoT devices to allow for inference of an output based on the input. For example, from a dataset of where, when, how and why people travel, AI could provide information to implement changes to infrastructure which could take a team of humans a great deal of time.
- Edge computing is the process of processing data at the network's edge rather than sending it to a datacentre or cloud compute unit, reducing the latency created by the increasing number of devices. Currently Edge Computing has been deployed alongside India's ITS' and AI-enabled cameras in Delhi to improve safety by detecting speeding vehicles, reducing the amount of accidents (*Kerala*, 2022)

How Does ITS Work?

Traffic Management Centres (TMCs) are at the core of ITS-enabled areas, being administered by a transportation authority. TMCs are used to collect and analyse data in order to optimise and control traffic in real-time. TMCs have 3 functions: Data Collection, Transmission and Analysis. (Choudhary, 2019)

- Data is collected by IoT devices such as Automatic Vehicle Identifiers, GPS based automatic vehicle locators, sensors, cameras, etc. These devices will record various information including traffic count, video surveillance, speed of vehicles, location, weight of vehicles, delays, etc. These IoT devices send all of their data to (usually) datacentres (if not using Edge Computing) to allow for analysis of the data collected.
- A major point of contention in ITSs is the transmission of data. As discussed previously, Edge Computing is the future of ITS data computation, due to its latency benefits, however most systems still use datacentres to process data, increasing latency due to the amount of data being received. Examples of transmission methods used could be traffic announcements over the internet, SMS or integrated car systems. Alternatively, even methods such as radio transmission or Continuous Air Interface Long and Medium Range (CALIM) depending on cellular connections and infra-red links.
- Once the data has been received at the TMC, it must be processed in stages:
  - Error Checking / Rectification: Checks for anomalous results or inconsistencies, identifies them and rectifies.
  - Data Cleaning & Synthesis: Data is formatted and altered, then pooled together to conform to analysis software requirements.
  - Adaptive Logical Analysis: After dataset is created, it can be analysed to predict traffic scenarios, available to be transmitted to respective systems, to deliver to users.

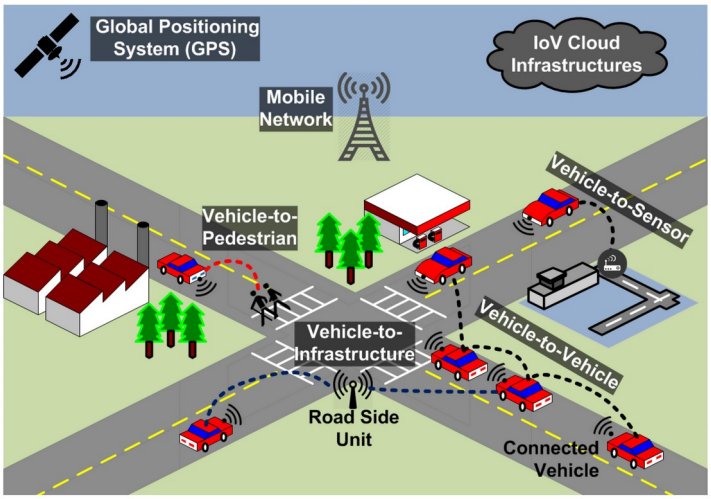

Figure 1: Smart cities communication architecture (Javed et al., 2016)

Users access this data using Travel Advisory Systems (TAS), which inform them on traffic and transportation updates, delivering real-time information such as travel time, traffic speed, delays, accidents, route changes, construction work, etc. This information can be access via various transmission methods including, but not limited to electronic signage (see Figure 2), radio stations, internet, SMS, and automated cell. A simple example of this is Waze, while not being an ITS-enabled TAS, it is functionally similar, the difference being users report the real-time information mentioned prior, available for other users to vote on it's accuracy to improve traffic and provide alternative routes to users in the event of issues on their journey.

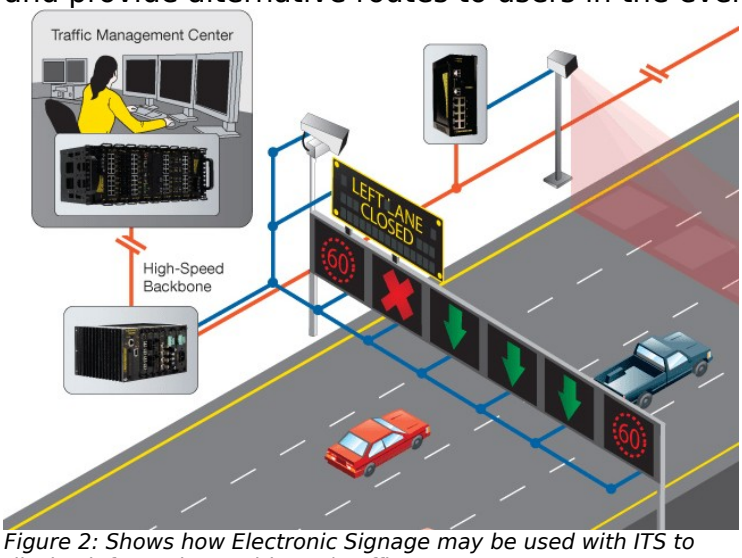

Figure 2: Shows how Electronic Signage may be used with ITS to display information to drivers.(Traffic Management System ::HOUSYS, n.d.)

Benefits of Intelligent Transportation Systems

Intelligent Transportation Systems have many benefits to millions of people living in potentially ITS-enabled smart cities. By using ITSs in conjunction with traditional technologies, we can integrate ITS devices into existing infrastructure and vehicles, allowing retroactive changes without the refactoring of technology use. The implementation of such technology would allow for maximally optimal routing of vehicles; assistance to drivers with collision avoidance with other vehicles; traffic management and control; traffic safety. (Leseu, 2024)

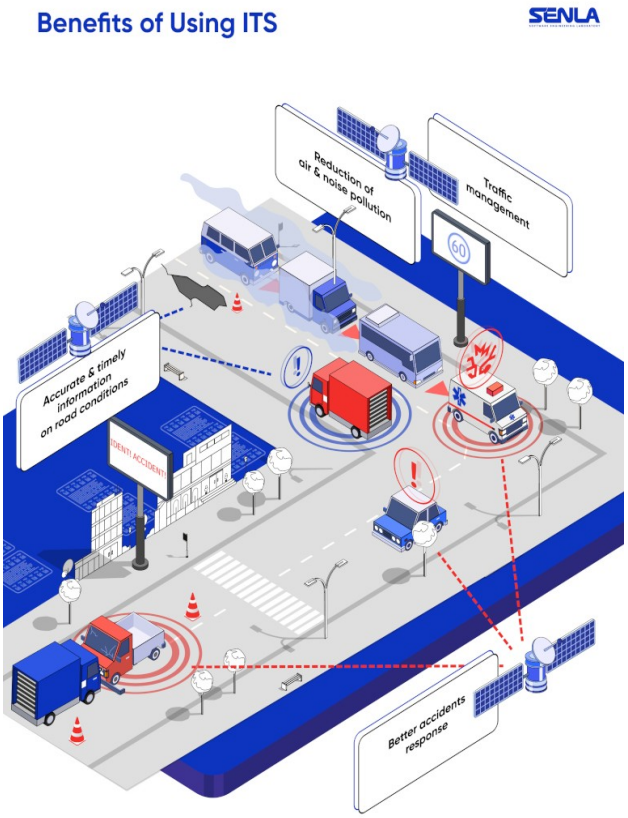

Figure 3: (Rather Large) Informative diagram describing in detail how ITS can be used to improve the safety and quality of life of drivers. (Leseu, 2024)

Improved Accident Management can help identify incident locations, warning drivers of potential congestion and reduce the risk of further traffic accidents, while informing drivers of emergency response on the road. According to the WHO, ~1.3m people die, and ~50m more are injured in road crashes per year – traffic accidents are the first cause of fatalities worldwide (Leseu, 2024). This could lead to millions of lives being saved by both reducing accidents in the first place, and also allowing first responders to more easily reach the drivers involved.

Improved Traffic Management help improve congestion by rerouting traffic based off sensor metrics or AI-enabled cameras, aiding in standstill traffic jams on motorways by routing traffic on alternative routes to their destination. This could help improve efficiency of delivery drivers where timely deliveries are essential to business and productivity, with an added benefit of ensuring maximum delivery times.

Additionally, environmental and financial benefits are created by the use of ITS, due to the reduction in standstill, start-stop traffic by calculating the minimum viable speed to keep traffic moving, minimising fuel consumption, and therefore car emissions. Due to this, ITS can help save drivers money on fuel.

One of the biggest benefits to ITS implementation is real-time road information for drivers, including potential road hazards like construction, roadblocks, inconsistent road surfaces / conditions, etc. ITS can also allow traffic authorities to provide information on disruptions or closures on driver’s routes.

Drawbacks and Challenges of ITS

Intelligent Transportation Systems are not without drawbacks however, high cost of implementation and maintenance, reliability issues and privacy concerns are not to be dismissed for the greater good, and compromises must be made.

The initial cost of ITS implementation would be very high; installing cameras, sensors, compute servers, even satellites on a scale of even a city would need critical evaluation. Maintenance of

these devices may also not be cheap, replacements, upgrades, repairs may require road closures on their own.

The use of cameras and other data collection devices continually recording drivers could present issues of privacy and ulterior motives, as their implementation is tame, but the potential for misuse of data is high. Although off-topic, I wrote an Extended Project (EPQ) in 2021 relating to Skynet in China for my A-Levels, and the widespread deployment of surveillance equipment, when misused, the data collected could be of potentially (subjectively) very detrimental consequence to a country's society.

The Future of ITS

Emerging and growing technologies in ITS such as 5G, AI and Blockchain mark the next age of traffic management and intelligent transportation.

5G alongside V2X communication allows for low latency, high bandwidth data transmission between vehicles and service applications, providing functions such as Platooning, allowing vehicles to operate in close proximity to eachother, form convoys and brake simultaneously. Benefits include improving emissions through reduced fuel consumption, and road capacity through reducing empty space on the road. Advantages as discussed previously also include collision detection and hazard warnings. (Salgarkar, 2024)

AI paired with Machine Learning Applications could allow for a wide range of applications such as traffic flow prediction, allowing forecasting of traffic in a small time-frame, saving commute times and delivery efficiency on the roads. The most obvious benefit of this would be Autonomous Vehicles, self-driving cars, allowing them to make real-time decisions. Each Autonomous Vehicle could generate up to 5TB of data per hour, emphasising the use of Edge Computing alongside these technologies too. (Salgarkar, 2024)

Blockchain will provide security benefits such as tamper-proof transaction records, decentralised legers, and self-executing contracts to ITS. By having a transparent, auditable system, transactions of participants, risk of fraud and corruption can be reduced, since blockchain is decentralised. By using cryptographic features, blockchain can protect sensitive personal data from bad actors using the system intending on attacking for personal gain. Smart Contracts can be implemented alongside ITS to further enhance security and data protection, as well as automation.

Conclusion

In summary, ITS can, and does revolutionise the transport industry, aiding in travel times, driver safety and efficiency. While implementation of ITS has it's challenges and compromises that must be addressed to reduce the risk of corruption and misuse of data, the benefits can massively outweigh the risks.

The requirement for investment for high initial cost, along with collaboration of organisations to provide infrastructure required for implementation would be the first major step in the next age of ITS-enabled cities. The technology and concepts exist right now, companies and governments must work together to deploy them in areas with high desire for increased safety and reduced congestion.

Imagine a city free of accidents and standstill traffic, where drivers can be sure of their arrival time, providing stress-free commuting and deliveries. Efficiency could be increased massively.

Section 2 – Network Practice

Task 1 – Routing

- Subnet A: 30 hosts → needs at least 32 addresses.
- Subnet B: 55 hosts → needs at least 64 addresses.
- Subnet C: 12 hosts → needs at least 16 addresses.
- Subnet D: 65 hosts → needs at least 128 addresses.

Network `86.30.88.0/21` (2048 Addresses):

- **Network Address:** `86.30.88.0`
- **Broadcast Address:** `86.30.95.255`
- **Usable IPs:** `86.30.88.1 to 86.30.95.254`

I have started with the largest subnet first to minimize the wasted space from subsequent subnets, and fragmentation.

Subnet D (Largest - 128 addresses)

- To accommodate 128 addresses: prefix /25.
- Subnet Mask: `255.255.255.128`
- Subnet Address: `86.30.88.0/25`
- **Usable IPs:** `86.30.88.1 to 86.30.88.126`
- **Broadcast Address:** `86.30.88.127`

Subnet B (Next largest - 64 addresses)

- To accommodate 64 addresses: prefix /26
- Subnet Mask: `255.255.255.192`
- Subnet Address: `86.30.88.128/26`
- **Usable IPs:** `86.30.88.129 to 86.30.88.190`
- **Broadcast Address:** `86.30.88.191`

Subnet A (Next largest - 32 addresses)

- To accommodate 32 addresses: prefix /27
- Subnet Mask: `255.255.255.224`
- Subnet Address: `86.30.88.192/27`
- **Usable IPs:** `86.30.88.193 to 86.30.88.222`
- **Broadcast Address:** `86.30.88.223`

Subnet C (Smallest - 16 addresses)

- To accommodate 16 addresses: prefix /28
- Subnet Mask: `255.255.255.240`
- Subnet Address: `86.30.88.224/28`
- **Usable IPs:** `86.30.88.225 to 86.30.88.238`
- **Broadcast Address:** `86.30.88.239`

Subnet	Network Address	Subnet Mask	Usable IP Range	Broadcast Address
Subnet D	86.30.88.0/25	255.255.255.128	86.30.88.1 - 86.30.88.126	86.30.88.127
Subnet B	86.30.88.128/26	255.255.255.192	86.30.88.129 - 86.30.88.190	86.30.88.191
Subnet A	86.30.88.192/27	255.255.255.224	86.30.88.193 - 86.30.88.222	86.30.88.223
Subnet C	86.30.88.224/28	255.255.255.240	86.30.88.225 - 86.30.88.238	86.30.88.239

- **Subnet C (12 hosts)** → Assigned to the network connecting **Router X** to **Host K**.
- **Subnet A (30 hosts)** → Assigned to the network connecting **Router X** to **Router Y and Host L**.
- **Subnet D (65 hosts)** → Assigned to the network connecting **Router Y** to **Host M**.
- **Subnet B (55 hosts)** → Assigned to the network connecting **Router Z** to **Host N**.

Subnet	Link	Network Address	Subnet Mask	Usable IP Range	Broadcast Address
Subnet C	X ↔ K	86.30.88.224/28	255.255.255.240	86.30.88.225 - 86.30.88.238	86.30.88.239
Subnet A	X ↔ Y ↔ L	86.30.88.192/27	255.255.255.224	86.30.88.193 - 86.30.88.222	86.30.88.223
Subnet D	Y ↔ M	86.30.88.0/25	255.255.255.128	86.30.88.1 - 86.30.88.126	86.30.88.127
Subnet B	Z ↔ N	86.30.88.128/26	255.255.255.192	86.30.88.129 - 86.30.88.190	86.30.88.191

- **Subnet C (12 Hosts)**:
  - Used for the connection between **Router X** and **Host K**.
  - Only 16 IPs (14 usable) are needed, which fits perfectly.
- **Subnet A (30 Hosts)**:
  - Used for the connection between **Router X**, **Router Y**, and **Host L**.
  - 32 IPs (30 usable) were allocated, which is enough for this subnet.
- **Subnet D (65 Hosts)**:
  - Used for the connection between **Router Y** and **Host M**.
  - Requires 128 IPs, which accommodates the need for 65 usable IPs.
- **Subnet B (55 Hosts)**:
  - Used for the connection between **Router Z** and **Host N**.
  - Requires 64 IPs (62 usable), which fits within the allocated subnet.

Subnet C: X <-> K (86.30.88.224/28, 12 hosts)

- **Network Address:** 86.30.88.224
- **Usable Range:** 86.30.88.225 - 86.30.88.238
- **Broadcast Address:** 86.30.88.239
- **Router X Interface IP:** 86.30.88.225
- **Host K IP:** 86.30.88.226

Subnet A: X <-> Y <-> L (86.30.88.192/27, 30 hosts)

- **Network Address:** 86.30.88.192
- **Usable Range:** 86.30.88.193 - 86.30.88.222
- **Broadcast Address:** 86.30.88.223

- **Router X Interface IP:** `86.30.88.193`
- **Router Y Interface IP:** `86.30.88.194`
- **Host L IP:** `86.30.88.195`

Subnet D: Y <-> M (86.30.88.0/25, 65 hosts)
- **Network Address:** `86.30.88.0`
- **Usable Range:** `86.30.88.1 - 86.30.88.126`
- **Broadcast Address:** `86.30.88.127`
- **Router Y Interface IP:** `86.30.88.1`
- **Host M IP:** `86.30.88.2`

Subnet B: Z <-> N (86.30.88.128/26, 55 hosts)
- **Network Address:** `86.30.88.128`
- **Usable Range:** `86.30.88.129 - 86.30.88.190`
- **Broadcast Address:** `86.30.88.191`
- **Router Z Interface IP:** `86.30.88.129`
- **Host N IP:** `86.30.88.130`

Task 2 – Routing Comparison Questions

Comparison of Default and Explicit Routes

A **default route** is an all-encompassing route, where any traffic that does not match any other route, is routed via the default route. In a priority list of routes, it would be considered as the lowest priority. Represented by `0.0.0.0/0` for IPv4 and `::/0` in IPv6, an example of a static route in Cisco IOS would be `ip route 0.0.0.0 0.0.0.0 10.0.0.1`, where all traffic's (`0.0.0.0`, netmask `0.0.0.0`) next hop would be `10.0.0.1`. The default route is easy to configure, and useful when dealing with unknown destinations, hence usually being used to direct traffic all to an upstream (ex. sending all traffic to ISP's router).

An **explicit route** (or **static route**) is kind of the opposite concept, rather than being comprehensive, it's specific and manual (almost like an override to the default route) defining where the traffic for a subnet should be routed to (the next hop). An example of this in Cisco IOS would be `ip route 172.16.2.0 255.255.255.0 10.0.1.1`, where the next hop of all traffic from the network `172.16.2.0/24` is `10.0.1.1`. In a routing table, this would be expressed as `172.16.2.0/24 via 10.0.1.1`. Explicit routes can offer more control over routing compared to default routes, as they 'explicitly' define the source of the packets to be routed via the next hop. Explicit routes are not always necessary, however they do have advantages such as preventing traffic from using the default route to ensure traffic gets routed to it's intended destination.

Comparison of Static and Dynamic Routing

Static and dynamic routing differ mainly in the way routes are maintained and configured. Static routing uses manual configuration of routes, carried out by the network administrator, which have fixed paths for packets to take. It benefits from it's simplicity on a small scale where topology would also be considered static. However, when dealing with changes to a network including link failures and new connections, a large client count can prove to be time consuming and labour-intensive due to the lack of scalability.

In contrast, Dynamic Routing uses protocols like BGP and OSPF to discover and maintain routes automatically. By having routers communicate with each other on an Autonomous System, they can exchange routing information to alter routes dependent on the network state dynamically in real-time. Due to this, Dynamic routing benefits from it's scalability and resilience to change;

network changes as listed prior can be dealt with without a network administrator intervening. However it’s complexity can make it more time-consuming to initially implement, and requires more performant hardware; improper configuration can also be more detrimental than static routing, leading to security risks

In conclusion, static routing is best suited in a small and unchanging network, emphasising simplicity and ease of control over routes, whereas dynamic routing is suited for large, complex networks where scalability is desired. However, they are not mutually exclusive, and many networks will opt for using both to leverage the advantages of either approach to routing.

Task 3 – TCP / UDP

Comparing TCP and UDP

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the two transport layer protocols used with the Internet Protocol (IP), and differ greatly with different use-cases to fit the needs and requirements of Application Protocols. TCP is connection-oriented, meaning a connection between two devices must be established before the transmission of data; this ensures a reliable, orderly and less error-prone packet delivery. Using methods such as three way handshakes, acknowledgments to confirm delivery, and retransmission for errored or missing packets, TCP is based on enforcing data to be the same as it originated as when it was sent. These features make TCP desirable for application protocols that require accurate and reliable transmission such as email (IMAP), file transfers (FTP) and web browsing (HTTP/S). The downside to TCP is that these error checking mechanisms, handshakes and acknowledgments all create overhead in transmission, allowing for less throughput, resulting in slower transmission speeds; TCP is less suitable for applications where speed is required.

In contrast, UDP is connectionless, meaning no prior arrangement is made between two devices, packets are sent without checking if the destination device is ready to receive them. It’s packets, named datagrams, are sent with no guarantee of delivery, order, or (error) state. This makes for a higher throughput, considerably increasing speed of transmission in comparison to TCP. Where UDP suffers however, is in it’s reliability; error-containing or lost packets are not error corrected or retransmitted, potentially making for incorrect data at the destination. These features make UDP ideal for applications where speed is more important than the final reconstruction of the initial data, such as audio / video streaming (although not used as much today with HLS / MPEG-DASH, WebRTC and RTMPS does use UDP for *live* video streaming), online gaming (WebRTC, Websockets, etc), and Voice-over-IP (VoIP).

However, many protocols may use both; developed by Google, QUIC is a network protocol that takes advantage of multiplexed UDP to replace the function of TCP with the aim to increase speed (by using UDP) and security (by incorporating TLS), and reduce latency. (Chromium, 2012)

In summary, TCP is commonly used where reliability, ensuring consistency of data, and order of packets is required, whereas UDP is commonly used in applications where speed and latency is required, and less emphasis is laid on consistency of datagrams. UDP for some uses is no longer the standard, such as with Video on Demand (VoD) streaming, ex. YouTube, since we now use protocols such as HTTP Video Streaming (HLS) to progressively download videos to the client. The use of TCP or UDP heavily depends on the requirements of the service / application being deployed, however the use of one or the other is not a requirement, they are not mutually exclusive and many applications may use both TCP and UDP over different ports to transmit different information.

Explaining the OSI Model

The Open Systems Interconnection (OSI) model is a conceptual framework that functions as a standard to network communication of systems. It divides it's process across 7 distinct layers, each with it's own purpose and responsibility to the transmission of data. Using this 7-layer process, the OSI model simplifies troubleshooting, development, deployment and the understanding of protocol purpose by isolating their purpose.

The OSI model functions in a descending order from the sender, or ascending to the recipient. Every layer provides a service to the layer above, and utilises the layer below. On transmission, it descends through the layers one-by-one, gaining metadata as it progresses. When receiving, data ascends, stripping the metadata as information is processed by relevant layers.

Layers of the OSI Model: (GeeksForGeeks, 2017)

- Application Layer (7)
  - User interaction with the network by utilisation of application services such as web-browsing (HTTP/S), email (SMTP), file transfers (FTP), etc.
- Presentation Layer (6)
  - By handling translation, encryption and compression, the Presentation layer ensures the data is in a suable format. Examples include SSL (Secure Sockets Layer) / TLS (**Transport Layer** Security) for web browsing, MPEG (Moving Picture Experts Group) for media encoding, etc. The Presentation layer is quite controversial for it's categorisation, since it does not always encapsulate protocols descriptively.
- Session Layer (5)
  - Handles the management and maintenance of connections between devices, including establishment and termination of sessions. Examples of which include the Point-to-Point-Tunnelling Protocol (PPTP), used for implementing (very basic) virtual private networks by encapsulating PPP packets.
- Transport Layer (4)
  - This layer categorises protocols such as UDP, TCP and QUIC, handling data delivery, error checking, segmentation and flow control dependent on protocol.
- Network Layer (3)
  - Managing routing and addressing using protocols like IP, ARP (based on implementation), ICMP and IGMP, this layer aims to determine routes for data to travel.
- Data-Link Layer (2)
  - Handling error detection / correction for transmission on physical links, it uses protocols such as Ethernet, PPP (Point-to-Point Protocol), ARP (based on implementation), to ensure data is sent to the correct device by their MAC addresses.
- Physical Layer (1)
  - The simplest layer, focusing on the physical connection between devices and the transmission of the binary data through a medium such as category cables, coaxial cables, radio waves, microwaves, etc. This generally includes the use of Network Interface Cards (NICs), cabled or otherwise.

Building on the function, the process when sending data begins at the Application layer, for example a HTTPS request is made in a browser. The HTTPS request is prepared, packaged, then addressed, descending the layers of the model. In Physical layer, the data is formed into electrical signals, light pulses, etc. and transmitted over the connection medium(s). When

received, this process is reversed, being unpacked and presented at the Application layer for the recipient.

The OSI model is important to promote interoperability and standardisations, allowing simplification of network design and troubleshooting, ex. connection issues in Physical Layer, address conflicts in Network layer. Unfortunately the OSI model is not perfect, many protocols cannot be categorised this strictly, namely from memory, SSL/TLS and ARP. TLS technically operates on the first 4 layers; ARP has been disputed as to whether it resides in the Data Link layer or the Network layer.

Conclusion

In this report, I have tried to write within the best of my ability, citing sources when used, although sometimes from notes and experience. I found Intelligent Transportation Systems to be quite applicable to my hobbyist level IoT and networking implementations and therefore rather interesting to discuss. In section 2, I think I have demonstrated my knowledge of subnetting a network the best I can. While I did not use many sources, I feel I have compared and contrasted, and explained the relevant technologies and concepts effectively. As anticipated, I also discussed the drawbacks of the OSI model, which was a point of research I did at A-Level out of confusion.

Disclaimer: **No AI tools were used for generating text**, only structure of the assignment ex. section headings and word count per section to remind me of word count, topic and some talking points; I have checked for remnants of my AI-generated structure and none should remain in my submission. Assignment is written in LibreOffice Writer using DejaVu Sans, font size 11 is used for all content, with font size 8 used for figure captions. Fonts **should** display fine across platform, but some characters have a (unlikely) potential to not display correctly on a windows computer. All citations cited correctly to the best of my knowledge, with my bibliography listed below in alphabetical order.

Bibliography

Andriy. (2024, September 4). *IoT in transportation: 8 examples of how it can improve the future | Vakoms*. Vakoms. https://vakoms.com/blog/iot-in-transportation-8-examples-of-how-it-can-improve-the-future/

Chipilska, I. (2023, September 14). *What Is An Intelligent Transport System And How Does It Work?* Modeshift. https://www.modeshift.com/what-is-an-intelligent-transport-system-and-how-does-it-work/

Choudhary, M. (2019, January 14). *What is Intelligent Transport System and how it works?* Geospatial World. https://geospatialworld.net/blogs/what-is-intelligent-transport-system-and-how-it-works/

Doan, T. (2023, October 23). *Exploring the Advantages and Disadvantages of Intelligent Traffic Systems*. Eastgate Software. https://eastgate-software.com/exploring-the-advantages-and-disadvantages-of-intelligent-traffic-systems/

GeeksforGeeks. (2017, August 30). *What is OSI Model | 7 Layers Explained*. GeeksforGeeks. https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/

Javed, M., Ben Hamida, E., & Znaidi, W. (2016). Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. *Sensors*, *16*(6), 879. https://doi.org/10.3390/s16060879

Kerala, India to Deploy AI to Reduce Traffic Violations – OpenGov Asia. (2022, April 28). Opengovasia.com. https://opengovasia.com/kerala-india-to-deploy-ai-to-reduce-traffic-violations/

Leseu, Y. (2024, January 8). *Intelligent Transportation System Importance - SENLA Company*. Senlainc.com. https://senlainc.com/blog/intelligent-transportation-system-importance/

Quan, N. (2023, March 27). *4 Technologies Enabling Intelligent Transportation System*. Eastgate Software. https://eastgate-software.com/4-technologies-enabling-intelligent-transportation-system/

QUIC, a multiplexed transport over UDP. (n.d.). Www.chromium.org. https://www.chromium.org/quic/

RantCell. (2024). Rantcell.com. https://rantcell.com/V2X-connected-cars.html

Salgarkar, R. (2024). *The Future of Intelligent Transportation Systems (ITS) Key Trends & Innovations*. Marketsandmarkets.com. https://www.marketsandmarkets.com/ResearchInsight/intelligent-transportation-systems-future.asp

The Evolution of ITS in the UK: A History. (2023, February 28). WJ Group. https://www.wj.uk/advice/history-intelligent-transportation-systems/

Traffic Management System ::HOUSYS. (n.d.). HoustonSystem. https://www.houstonsystem.com/solutions-2/transport-management-solutions/traffic-management-system/

V2V Communication: Cars communicating with cars? | Dalroad. (2022, November 4). Dalroad. https://www.dalroad.com/resources/v2v-communication-cars-communicating-with-cars/