Marking Rubric

Mark	10	5	0
Idea potential	The idea has great potential and is very well suited for a research project. The idea reflects the current state of the art and represents potentially a hot topic from an emerging research or technological field. The idea reflects the student's programme of study and builds on existing competencies and modules taught and delivered within the programme.	The idea has good potential and is suited to develop as a research project. The idea stems from a well-known area that is well understood and there is a large amount of existing work in the area. The idea reflects the programme of study and builds on existing competencies and modules taught and delivered within the programme.	The idea is not suited for a research project. The idea does not demonstrate any level of ambition and/or is unrelated to the programme of study.
Research Context	The motivation and narrative for the research is very defined and articulated. The high level topic is very well described and challenges related to the topic are specified and detailed. The research context is easy to read and flows logically. The proposal clearly identifies where the contribution fits into existing work in the area. Existing work is appropriately cited and references are included. References are appropriate and are properly specified and the reader is convinced that a comprehensive review of the area was conducted. The student has demonstrated a high level of critical thinking when developing the research context.	The motivation is embedded in the text but sometimes it can be difficult to extract when reading the proposal. The topic does describe some of the challenges in the area but these are not placed in context to the idea. The context reads like a background to the area rather than a critical analysis of where the proposed project fits into the field. Citations are included but the reader is not convinced that a comprehensive review of the area is conducted. Some/most of the references are web references from sources that are not peer reviewed or are proprietary in nature.	The research context does not demonstrate any level of critical analysis and reads more like a proposal that would be presented at undergraduate level.
Aim	A simple statement that refers to the main goal of the project is defined. This goal relates and is developed bearing in mind the research context presented. The aims demonstrate some ambition and are appropriate to the level sought.	A research aim has been defined that relates somewhat to the research context presented.	Research aim is not appropriate to the level sought i.e. MSc. The aim is not related in any way to the context and motivation included as part of the proposal.
Objectives	The research objectives are well defined and constructed correctly. An appropriate number of research objectives/questions have been defined. The research objectives relates to the research context and identified challenges in the field. The research objectives are realistic and are within the scope of the project.	The project proposal may have defined too many objectives and may be presented incorrectly. They objectives are ill defined and only somewhat related to the context presented. Some of the research objectives lack ambition and outline questions that may be clearly answered without undertaking a research project.	The questions/objectives are ill defined, lack ambition and are do not align with a level 9 masters project. The research questions read like what you would expect at an undergraduate level.

Example 3

Project Title

A Secure Software Defined Wireless Sensor Network

Marking Rubic	
Example Number:	
Idea potential	
Research Context	
Aim	
Objectives	

Research Context

The Internet designed in the 1970s was conceived to support an open “network of networks” represented by academic, government and research communities, all of which use a common set of communication standards. Since 2004 (which was the year that the speed offered by fixed broadband exceeded that from using dial up), the number of individuals using the Internet has grown from 1 Billion in 2004 to 3 Billion in 2015. These numbers are expected to increase further with the interconnection of smart objects and "things" communicating via a common platform i.e. the Internet. These "things" are expected to drive the Internet to the edge of its architectural capability and capacity and are creating new engineering requirements for the Future Internet (FI). "Tussle networking" is one of these requirements where the heterogeneous nature of devices, networks, technologies and communication protocols are considered essential to support. However, the ossification of the Internet has limited it ability in meeting these requirements as stakeholder agreement is required before any change can be applied over the Internet's network of networks.

Network Virtualization has been adduced as a technology to create the Future Internet (FI) as it leverage's the existing infrastructure foundation of the Internet, while at the same time supporting heterogeneous devices, networks and communication protocols. Dissimilar from the current Internet, network virtualization separates service provisioning from data transportation mechanisms by uncoupling the Internet Service Provider (ISP) into two separate entities, Infrastructure Providers (InPs) and Service Provider's (SPs). Within this environment, Virtual SPs (VSPs) can broker a slice of virtual instances spanning a set of physical resources, consisting of links and nodes, across multiple heterogeneous InPs to create their own Virtual Networks (VNs). In the virtualised network environment InPs can be any type of provider that can expose their network resources through the use of programmable interfaces [v].

Much of the research completed to date in the area of network virtualization and the FI focus on InPs in wired and wireless networks. More recently, applying virtualization to Wireless Sensor Networks (WSNs) has been proposed proposed by Jayasumana et al [i] and by Leontiadis et al. [ii]. Extending the FI vision to include WSNs allows the evolution of sensor networks in their current manifestation, as isolated and application specific deployments. In this evolved view, the sensing abilities of WSN nodes can be shared among various federations and composed to form new applications and services beyond its original purpose or design. Separating the network infrastructure and its ownership also means that the traditional benefits associated with virtualization can also be leveraged in WSNs. These benefits include economies of scale, reduced cost of ownership and reduced cost to customers.

A key enabling technology to support network virtualization is Software Defined Networking (SDN) [iii]. SDN separates of the data and control planes in the network, creating a vendor agnostic forwarding abstraction through the definition of general ''match + actions'' that the switch understands. SDN, and

its implementation OpenFlow [iv] introduces a centralized controller to manage the behaviour of the entire network. The centralized view of the network that SDN provides offers the potential to innovate network service provisioning allowing the ability to dynamically adapt to the Quality of Service (QoS) requirements of user applications. Within the SDN architecture, northbound and southbound interfaces are defined. The southbound interface refers to the interface between the programmable switch layers (SDN capable switches) and the software controller, with communication at this interface enabled by the OpenFlow [iv] protocol. The northbound interface on the other hand focuses on the: expression, definition and translation of network policies into a form that the controller can understand and act upon; and Application Programming Interfaces (APIs) that are used to communicate between the controller and the services running over the network (see Figure 1). SDN in its current form is largely targeted towards LAN/MAN/WAN environments consisting of switches, routers, firewalls and various middle-boxes.

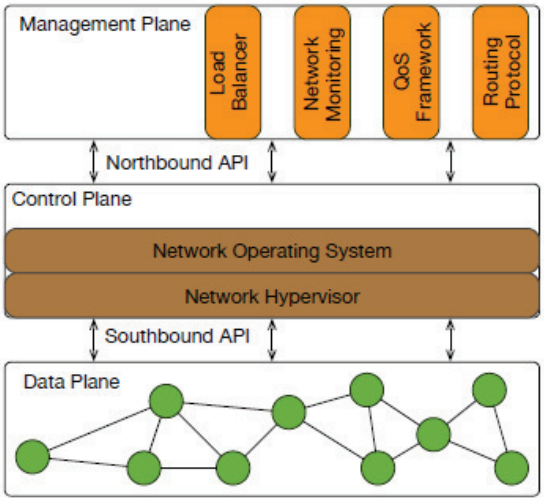

Figure 1 SDN Controller Architecture

Applying SDN to WSNs however, represents a very different environment from what SDN was originally designed for in enterprise networks: low data rates, low performance and unreliable links. Several challenges exist in applying SDN to WSNs and one of these challenges is in the area of security. Addressing this challenge is critical to ensure adoption of the technology by InPs willing to offer their infrastructure to form part of VNs leased to various SPs and by SPs who want to ensure that their networks are isolated from other tenants on the same underlying infrastructure. Isolation is necessary to ensure that requirements of fault tolerance, security and privacy are met and misconfigurations in one VN do not affect other coexisting VNs [v]. In order to provide a secure framework for Software Defined WSNs confidentiality, integrity, isolation and authentication areissues that need to be considered. These security challenges are further outlined below [vi, vii, viii]:

1. **Northbound layer:** The programmability aspect of SDNs through the northbound interface and its respective APIs makes this interface vulnerable to malicious code exploits and attacks. In addition, conflicts may emerge between policies defined at this layer which would impact the operation of the entire network. There has been numerous contributions in the area of enforcement of security policies have which most notably include Son et al [ix] who defined a model checking engine called FLOVER that verifies flows against network security. In addition, Wang et al [x] proposed an approach to identify and resolve security conflicts in the SDN firewall, achieved by searching the

flow paths against firewall rules to determine conflicts. Kreutzer et al [xi] outlines a comprehensive view of contributions in this space.

2. **Controller layer:** The centralized controller provides a central network model which can be used to provide optimal resolution over a number of WSN constraints which include minimizing: latency and packet loss; and maximising the lifetime of the network by optimally distributing load among nodes. This central network model if exploited could be used in attacks with the aim of reprogramming the entire network. In addition, the centralized controller has the obvious drawback of being a single point of failure in the network and is particularly vulnerable to Denial of Service (DoS) and security threats. Both of these attacks could comprise the operation of the entire network as the SDN controller has control over the network in its entirety. The control logic of the SDN controller would need to be enhanced so that it is cognizant of the constraints of the underlying resources when applying security to the WSN infrastructure. Existing security enhancements for SDN include: FLEXam [xii] that samples packets stochastically considering the application requirements to reduce the flow setup time and reduce control plane load; CloudWatcher [x] which monitors Cloud environments and; Learning-Intrusion Detection System (L-IDS)[xi] a security service embedded to protect mobile devices. None of these enhancements are relevant to WSNs.
3. **Southbound layer (Transport layer security):** Within enterprise networks an out-of-band channel is used between the controller and each switch, and secure tunnels are leveraged to take advantage of the high data rates. [xiii] identified that the lack of adoption of TLS by major vendors implementing SDN exposes the network to DoS attacks and fraudulent rules in the network. Out-of-band channels could also be used in WSNs using dedicated higher power radios, but that would increase the energy cost. A mechanism to provide secure energy efficient transport layer security for WSN need to be considered to (a) prevent the insertion of fraudulent rules (b) modification of rules in the WSN nodes (c) secure authentication of nodes and (d) prevent side channel attacks.
4. **Data Plane Layer:** Within a WSN data is its main commodity. To protect this commodity the: sender of the data needs to be authenticated; and mechanisms need to be put in place to ensure it is only sent to its intended recipient to ensure confidentially. Data integrity and freshness are also key requirements. However, due to the inherent nature of WSN themselves many challenges exist to ensure the security of the data in WSN [xiv, xv, xvi]. Attacks to WSN range from: attacks against privacy which is normally performed through eavesdropping and camouflage; Denial-of-Service (DOS) attacks as a result of signal jamming or violating the communication protocol in use; sybil attacks where a "malicious device illegitimately takes on multiple identities" [xvii]; node replication; and traffic analysis attacks. To prevent rule modifications and subsequent modification of data packets transport layer security is vital to support.

At the data plane layer of WSN it is important to recognize the unique difference between nodes in enterprise networks and WSN. In enterprise nodes i.e. switches only performing switching functions, whereas WSN nodes perform switching functions but also run applications that perform sensing operations such as environmental monitoring. In virtualized WSNs, the sensing applications can be shared by multiple tenants or SPs and so application layer security at this level needs to be considered to prevent malicious code exploits and attacks that would impact the operation of the entire network.

Research Aim

The work described above illustrates that the major contributions in the area of SDN security has been based on security enforcement policies and security enhancements for wired networks with a focus

on broad mechanisms for security. None of the contributions consider: data plane devices as nodes in WSNs; and the unique challenges in virtualizing and securing WSNs using SDN as an enabling technology. Based on the above it is the aim of this proposed project to create a secure virtualised framework for WSN that considers in particular the controller layer of SD WSN environments.

Research Objectives

The objectives of the research are as follows:

- To examine whether SDN improves the security posture of a WSN environment.
- To determine what attacks a software defined WSN is particularly vulnerable to.
- To explore the impact of creating a secure virtualised framework for WSN in terms of network lifetime.