Securing Autonomous Networks through Virtual Closure

Darren Hurley-Smith[1], Jodie Wetherall[2], Andrew Adekunle[2]
University of Kent[1], University of Greenwich[2], United Kingdom

Abstract

The increasing autonomy of Mobile Ad Hoc Networks (MANETs) has enabled a great many large-scale unguided missions, such as agricultural planning, conservation and similar surveying tasks. Commercial and military institutions have expressed great interest in such ventures, raising the question of security as the application of such systems in potentially hostile environments. Preventing theft, disruption or destruction of such MANETs through cyber-attacks has become a focus for many researchers as a result. Virtual Private Networks (VPNs) have been shown to enhance the security of Mobile Ad hoc Networks (MANETs). VPNs do not normally support broadcast communication, reducing their effectiveness in high-traffic MANETs which have many broadcast communication requirements. To support routing, broadcast updates and efficient MANET communication a Virtual Closed Network (VCN) architecture is proposed. By supporting private, secure communication in unicast, multicast and broadcast modes, VCNs provide an efficient alternative to VPNs when securing MANETs. Comparative analysis of the set-up and security overheads of VCN and VPN approaches is provided between OpenVPN, IPsec, Virtual Private LAN Service (VPLS), and the proposed VCN solution: Security Using Pre-Existing Routing for MANETs (SUPERMAN).

1. Introduction

Interest in swarms of autonomous UAVs is growing rapidly, with civilian and military authorities spearheading initiatives that will see the deployment of many aerial mobile nodes capable of self-control and self-guidance on a wide range of missions [1]. A key issue of such projects is the security of the communication required for inter-swarm communication. Autonomous systems require a large amount of communication to operate, before even considering any swarm-to-base communication requirements [2]. As a result, secure Mobile Ad hoc Network (MANET) communication has become a key topic for discussion, where autonomous activity is seen as desirable.

Virtual Private Networks (VPN) provide a means for nodes to communicate securely and privately over an otherwise insecure medium. Traditionally, such networks have operated over the Internet with the assumption that due to the variable routes and dynamic topology, the lines of communication cannot be trusted. More recently, this philosophy has been applied to Mobile Ad hoc Networks (MANETs).

MANETs typically use wireless radio communication as their transmission medium. Due to the inherently broadcast nature of typical radio transceivers, the medium can be assumed to be insecure. This is known as the open-medium problem; the medium itself is observable by third-parties in range and is therefore insecure unless steps are taken to prevent trivial observation of communication.

VPN approaches have been used to secure MANETs, VPLS most notably for its mesh-based approach to the formation of a secure network over insecure infrastructure. IPsec [3] and OpenVPN [4] have also seen use in MANETs comprised of roaming nodes, allowing communication over third party wireless infrastructure between nodes when they move out of range of each other. In all such cases, the emphasis has been on point-to-point communication; in which nodes are expected to communicate on a 1:1 basis.

Virtual Closed Networks (VCN) deviate from the VPN philosophy in two key areas; behavioural control of communication and hierarchical provision of security. VCN nodes must submit to a common set of communication behaviours. Deviation from these behaviours mark a node as an imposter, or malicious node. All communication outside of the expected set is ignored, and the malicious node is denied access to the network.

This paper investigates the efficiency of the VCN approach, when compared with a selection of VPN protocols. The security features of the VCN and VPN approach are compared in qualitative discussion, while the costs associated with securing a MANET using OpenVPN, IPsec, VPLS [5] and Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN) are analysed using the quantitative results of simulation.

2. Literature Review

2.1. Autonomous MANET Security Considerations

The primary concern for any MANET using wireless communication, is the open-medium problem [6]. The problem is characterised by an insecure communication medium; a means of communication that can be trivially observed and interfered with, with no ability to directly protect the medium against such attacks. The open-medium problem means that any communication between nodes in a MANET must be assumed to be insecure by its very nature, requiring that steps be taken to ensure confidentiality, integrity and authentication.

2.1.1. Vulnerabilities. The first key weakness exposed by the open-medium problem is that of observable communication. Passive attacks against networks are a common precursor to more aggressive cyber-attacks. Eavesdropping on communication, recording data and mapping the topology of a network from the outside are all possible if a malicious observer has unfettered access to information flowing through the network. Such information must be protected to ensure that malicious observers are not able to steal identifying information or critical information about the nature of the mission being undertaken by the network.

A second stage of attack is likely, should sufficient information be gathered [7]. Impersonation, Sybil, wormhole and black hole attacks depend on a certain critical mass of data being accumulated to allow malicious nodes the ability to fool legitimate nodes into believing that the malicious nodes are members of the network [8].

Such attacks are referred to as active attacks, and they directly impact on network attributes, such as quality of service and reliability. They frequently compromise related functions of the network, such as the application layer requirements of communication; the ability to communicate mission-vital information or control associated functions in a distributed fashion. By compromising communication in a MANET, an attacker can disrupt or destroy the associated functionality of the network.

2.1.2. Securing the network. ITU-Rec X.805 outlines the security threats to wireless networks and associated defences against such threats. Five threats are identified, and eight solutions are proposed to counter them. The five threats are; destruction, corruption or modification of data, theft or removal of data, disclosure of information, and interruption of services [9].

The proposed counters to these threats are; access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy. It is possible that only some of these security services are required. For example; non-repudiation is only required if interruption of services is anticipated. However, it must be noted that in long-lived MANETs, operating without human control, full-suite security is preferable due to the inability to predict the nature, form or intent of a cyber-attack that occurs in the field.

Table 1 highlights the identified security threats and their solutions.

Table 1. ITU-Rec X.805 mapping of threats to security solutions

	Loss	Mod.	Theft	Disclose	Denial of service
Access control	☑	☑	☑	☑	
Auth.			☑	☑	
Non-repudiation	☑	☑	☑	☑	☑
Data confidence			☑	☑	
Comm. security			☑	☑	
Data integrity	☑	☑			
Available	☑				☑
Privacy				☑	

2.1.3. The implications of service interruption, disclosure or corruption. In an autonomous MANET a means of allowing nodes to collaborate and avoid workload duplication is required. Consensus Based Bundle Algorithm (CBBA) [10] and it is clustered contemporary, CF-CBBA, are algorithms that provide such services [2].

Although these algorithms can provide the means for a MANET to perform complex task collaboratively and efficiently among their constituent nodes, they are not secure. They are collaborative applications, requiring a great deal of communication between networked nodes even in the most efficient of configurations. As a result, they are vulnerable to the interception of mission critical data.

Over a wireless medium, this is a readily apparent problem. Passive attackers may derive information about the whereabouts (or destination) of nodes, allowing the planning of theft or physical compromise of nodes. Destruction of data may slow or prevent the task allocation process reaching convergence, consuming resources wastefully. More subtly, corruption of that data may allow an attacker to decide where nodes go, facilitating theft, physical compromise or allowing the pursuit of other surreptitious goals that require that the autonomous MANET be manipulated, but not prevented from functioning.

With these issues presenting a very real threat to the efficiency, sanctity and ability of the network to perform its task, it is apparent that security must be applied to ensure that task allocation is protected from attack.

2.2. Virtual Private Networks

VPNs represent a class of network that operates in a pessimistic state. Unlike naive MANET implementations, where the medium is assumed to be trustworthy and all node benevolent, VPNs assume that the medium is insecure, and that the network is subject to observation and attack at any moment.

Privacy is the core philosophy of the VPN. VPNs were initially intended to protect the privacy of communication between end-points over unsecured mediums, such as the Internet. Some point-to-point implementations have been proposed, though these are usually limited in scope (closely situated collections of trusted nodes) and are more akin to VCN architectures than traditional VPN architectures [11].

OpenVPN is an open-source application developed to secure communications between machines in separate locations, over a potentially insecure link [12]. It is capable of traversing multiple network domains and makes use of the OpenSSL and TLS standards for certificate exchange, or pre-shared key-based approaches to authenticating legitimate members of the VPN. This is further enhanced by the addition of user-selected passphrase insertion to the SSL/TLS authentication process, should the user select this option.

VPLS adds multicast (and in some cases broadcast) functionality, emulating Ethernet functionality to extend the ability to address all members of the VPN despite their disparate geographical locations and variable routes (which VPLS does not track or maintain). Due to the added complexity of maintaining a LAN emulation over potentially insecure infrastructure, a full mesh is required [13]. This means that all nodes must be connected to all other nodes. That may be over n-hops, but all nodes must have a viable end-to-end connection to all others to participate in the network. Although useful for MANET implementations, where broadcast functionality is highly desirable, the additional memory overhead and connectivity requirements can be a problem in networks with an unreliable communication medium. VPLS has been secured using modified Host Identity Protocol (HIP) Base Exchange (BEX) [14].

IPsec is a suite of protocols intended to provide secure end-to-end communication between nodes in a network. IPsec is typical of VPN philosophy, in that it provides end-to-end security between nodes, but plays no role in point-to-point security and relies on secure routing to protect data in transit. It extends confidentiality, integrity and authentication services to mutually authenticated end-points, but does not provide MANET-specific support. MANET implementation, such as MANIPSEC have been shown to improve the performance of IPsec and extend multicast capabilities to communication using IPsec over MANETs, but the intensive key-exchange and authentication mechanisms continue to represent a substantial overhead for resource-limited networks [15].

3. Virtual Closed Networks

VCNs differ from VPNs, in that the focus is on the network, not the links that form it. VPNs seek to protect instances of communication between nodes in a network, they define a series of secure links between nodes, with may be 1:1 or 1:N in nature [16]. However, the focus is set on the links, the network topology, access control policy and communication medium play no role in defining the VPN. VCNs adhere to a holistic core philosophy. They are intended to provide security by closing the network against outside interference, both end-to-end and point-to-point.

A VCN will extend protection beyond confidentiality, integrity and authentication, by providing services that ensure routes are secure. This provides weak guarantees of delivery; weak due to the fact that medium-control is not a part of most VCNs, and so disruption of the communication medium may still cause loss of data. However, such loss will not be driven by the inclusion of malicious nodes in the routing process; a VCN will not tolerate unknown propagation of packets unless specific white-listing of message-types is included in the security definitions it adheres to.

Figure 1 shows a grouping of twelve MANET nodes, all of which are members of the same network. All nodes have secure end-to-end connections with each other, forming a VPN. In a VPN, the links on the route to a destination are unimportant, security services are applied to the packet and the route is trusted to propagate it towards a destination. As a result, the trustworthiness and reliability of each node on a route are unimportant to the VPN.

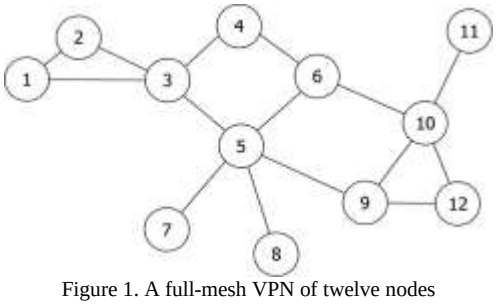

Figure 1. A full-mesh VPN of twelve nodes

MANET nodes must assume the role of router and end-point to maintain a viable network. As a result, the intermediate nodes in a route cannot be assumed to simply route messages between distant nodes; they have the capability to act on received data, storing it or relaying it to third parties. End-to-end communication may be secure, but the incorporation of untrusted nodes into the routing process represents a significant security risk in the long term. It must be noted that unless a secure routing method is selected for the MANET, routing will be insecure; allowing any nodes with the appropriate suite of protocols to participate. For example, Ad hoc On Demand Distance Vector (AODV) [17] will allow any responding node also using AODV within the defined address space to participate in routing, allowing potential attackers to be incorporated into the network topology directly. This applies to any unsecured routing protocol.

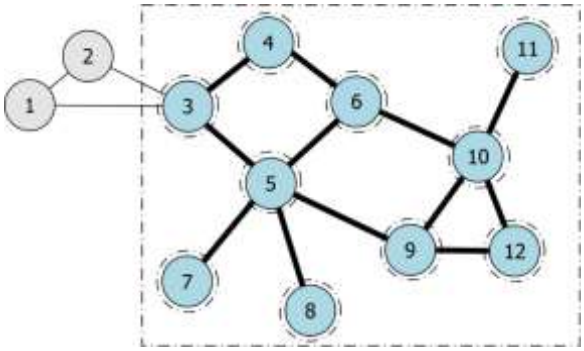

Figure 2. A full-mesh VCN of ten nodes with two non-member nodes in communication range

Figure 2 shows an abstraction of a VCN. Ten nodes are in the VCN (blue nodes), while two (the grey nodes) are not. Being in a VCN means being recognised by the network as a legitimate member node. Appropriate confidentiality, integrity and authentication protocols must be applied across all node, both end-to-end and point-to-point for a MANET to be considered to be a closed-network.

Member nodes may only communicate with each other securely; they will not trust grey nodes to propagate their traffic intentionally (though it may still be received). The rectangle boundary around the network represents the virtual element of the closure of the network. This is an abstraction of closure; the actual closure is performed on each node. Because of this, the heavy black lines between blue nodes represent that they must be neighbours to uphold the protocols keeping the network closed against outside intrusion.

VCNs are not as far-reaching in scope as VPNs, due to this tightly-knit security approach. A VCN may use a VPN to communicate over unreliable infrastructure to reach another VCN, end-point or designated network of another type, as an extension of its communication. Alone, a VCN closes the target network against outside observation and interference at the node level. By ensuring all nodes adhere to the same security protocols, even the most distributed network may protect itself in a unified manner, mitigating the effects of an open communication medium by ensuring that observers may only obtain encrypted data, and are refused participation in the routing of such information.

4. SUPERMAN: A Novel VCN

Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN), is a novel security framework that, at its core, represents a VCN approach to MANET security. The development of SUPERMAN was driven by the need for autonomous UAV networks; resource limited networks comprised of lightweight nodes. Such networks have specific communication requirements; they require frequent communication to self-organise and distribute tasks, they require security to ensure that mission-data and network-data are not obtained or modified by malicious parties, and they must do both as efficiently as possible, due to the limited bandwidth.

To ensure that all of these needs are met, a VCN approach has been proposed. Key to this approach, is the ability to authenticate new nodes and ensure that the network may accept new members and deprecate nodes as the need arises. This need is driven by the application in question; for example, a surveying task using Unmanned Aerial Vehicles (UAVs) with a mission duration longer than the UAV's maximum flight time. This would require that nodes (the UAVs) to be replaced in the deployed network as they need to leave to recharge and are replaced by new nodes.

4.1. Establishing Secure Networks

SUPERMAN uses a certificate-based approach to authenticate new nodes and allow them to become members of the network if they have the appropriate credentials. Once authenticated with the network, a node will begin to form secure links, by associating itself with other member nodes on-demand. It is at this point that knowledge of the state of nodes on a route becomes important.

Nodes may participate in routing once they have become members of the network, using network-wide keys for broadcast communication. They must securely associate with each other to communicate in a unicast or multicast manner. A SUPERMAN node must exchange a key-share with other nodes and perform Diffie-Hellman key exchange to generate appropriate keys for end-to-end and point-to-point cryptographic functions.

SUPERMAN nodes will not propagate such information along routes with non-member nodes, and no intermediate node in the route will propagate the security data to a neighbouring node it isn't securely associated with. If nodes are network members, and are securely associated with each neighbouring node, the propagation of security credentials between end-points can begin. Security associations are formed on demand, when a source node requires direct communication with another which it doesn't yet have security associations with.

Due to the potentially large number of nodes in a SUPERMAN network, and the large amount of security associations that must be formed during the course of a mission, measures have been taken to reduce the communications overhead associated with this phase of security set-up.

4.2. Efficient Node Association

In VPN systems like IPsec, VPLS and OpenVPN, nodes will associate over an undetermined number of nodes in a route. It does not matter if these nodes are members of the VPN or untrusted infrastructure, the exchange of credentials occurs over the full length of the route.

SUPERMAN employs a delegated authentication method to reduce the effective length of routes in the VCN, if possible. On request of a destination nodes key-share, if the route between the two nodes includes one or more nodes that have previous associated with the destination of the security association request, the first along the route with the destinations key-share will reply to that request on behalf of the destination, instead of forwarding the request along the route. This has the effect of shortening the length of the route between source and destination nodes during security association. This is possible as each SUPERMAN node maintains a security table of key shares associated with each node it has previous associated with. As keys are unique to the link between two associated nodes, delegated authentication does not allow the delegate node to form a key on behalf of the associating pair, instead, it merely passes on the required key share to allow the end-points to generate the cryptographic keys required to secure their communication link. This method allows for the expedient, efficient sharing of security information in a safe, robust manner. By allowing nodes to exchange the credentials of nodes they have securely associated with, the cost associated with exchanging authentication information securely over the full length of the route as one must in a VPN is mitigated.

4.3. Security Overhead

In addition to establishing a secure network, a VCN must protect data communicated over it. As VCN protocols, such as SUPERMAN, are implemented at the network layer as an integral element of the network interface itself, the VCN security elements can be inserted prior to the addition of header data.

This also means that SUPERMAN packets only require one IP header, instead of requiring that an existing IP packet is encapsulated within a VPN packet with an additional IP header. As a result, the packet size is reduced when compared with many VPN protocols.

This feature of the VCN approach provides low cost security, and avoids data duplication. It does not reduce the protection provided to the data packet, confidentiality is guaranteed end-to-end and point-to-point. In addition, authentication is assured at each hop and between destination and source.

5. Methodology

5.1. Hypothesis

It is hypothesised that the SUPERMAN VCN approach to secure MANET communication will provide a more efficient (less costly per node) set-up than its VPN equivalents. VPLS should benefit from its multicast capabilities in the latter link-securing stage of the security set-up process, relative to IPsec and OpenVPN. However, SUPERMAN should outperform all three VPN approaches, by ensuring that all nodes in the network may be trusted, and using this knowledge to allow the use of delegated authentication to reduce the effective distance between non-neighbouring nodes that must form a secure end-to-end link between themselves.

5.2. Simulation Parameters

Simulation is undertaken using MATLAB. IPsec, OpenVPN, VPLS and SUPERMAN are simulated to allow comparison of their end-to-end authentication and key generation communication. The number of communication events (transmissions, assumed to be within MTU) and number of bytes transmitted are recorded, reported and analysed. Table 2 outlines the simulation parameters for the experiments.

The simulated network is a MANET of 10-100 nodes. The network is fully connected, with a hop count of 5 setting the maximum boundary for the length of routes between nodes. Where required by the selected VPN protocol, node ID 1 is selected as the server for VPN authentication protocols.

Table 2. MATLAB simulation parameters

Number of Nodes:	10 - 100
Routing Algorithm:	Dijkstrka [18] (shortest path)
Number of Iterations:	50
Simulation Area:	100m x 100m
Communication Range:	50m
Max Hop Count:	5
Random Seed:	11
Key Share Size:	128 bytes
Certificate Size:	1013 bytes

Due to the differing capabilities of the three VPN approaches selected for this comparison, two experiments have been devised, both adhering to the settings outlined in Table 2. It is assumed that the network suffers no loss or packet corruption.

5.2.1 Network authentication. This experiment involves the authentication of nodes with the network itself. IPsec and OpenVPN do not extend network authentication functionality, being focused on client-server and client-client pairings for secure tunnel formation.

SUPERMAN and VPLS, set up a network within a network, instead of just forming peer-to-peer links over an untrusted medium (the internet in the case of most VPN). This has the added benefit of allowing multipoint connectivity. As a result, both approaches require that nodes authenticate with the network.

SUPERMAN nodes must authenticate with each other using certificates issued by a trusted authority. This trusted authority is only required during initialisation, and when certificates need to be updated.

VPLS designates a central server that authenticates nodes and equips them with unidirectional (initiator and responder) keys common to the broadcast virtual Ethernet mesh used for VPN communication. VPLS does not extend services to routing, it is assumed that routing will take place without VPLS securing those routes. All routes are pre-generated for VPLS, whereas SUPERMAN will only begin routing once nodes have authenticated with the network (receiving broadcast keys in the process).

This experiment involves the comparison of VPLS and SUPERMAN network authentication communication, analysing the number of communication events and bytes transmitted to achieve full network authentication.

5.2.2 Key negotiation (end-to-end). SUPERMAN, OpenVPN, IPsec and VPLS all secure tunnels between nodes. This is the primary function of all four approaches, though SUPERMAN and VPLS extend further network authentication procedures to facilitate more complex use of network topology during communication over secure tunnels.

All four approaches are simulated forming secure tunnels between all nodes in the target network. This is assumed to be performed in an isolated environment with nodes only communicating security information during this process; no ancillary communication can occur until the process is complete. The number of communication events and amount of data (in bytes) required by this process is compared to highlight the differences between the VPN protocols selected and the SUPERMAN VCN framework.

5.2.3 Secure task allocation. Task allocation is an example of a highly distributed, autonomous application used by mobile nodes. Consensus Based Bundle Algorithm (CBBA) and Cluster Form CBBA (CF-CBBA) are examples of task allocation algorithms [2]. They provide a means by which groups of nodes can collaborate autonomously, performing complex tasks as a team. As a result, they have been chosen as the representation of an ongoing, vital application.

Such applications require security to ensure that they reach a solution that is agreed upon by all participating nodes. They also require protection against modification of data, to ensure that no malicious factors are allowed to affect the outcomes of the task allocation process. VPN and VCN services can provide that protection.

Table 3 defines the simulation parameters for this experiment.

Table 3. MATLAB simulation parameters

Number of Nodes:	18
Cluster Configurations:	CBBA: 18 nodes (no clusters) CF-CBBA 1: 3 clusters of 6 nodes CF-CBBA 2: 6 clusters of 3 nodes
Number of Iterations:	50
Simulation Area:	100m x 100m
Communication Range:	50m
Max Hop Count:	5
Random Seed:	11
Number of Tasks	1-50

Eighteen nodes are tasked with a simple mapping problem. They must travel to randomly generated waypoints, represented by tasks. Nodes must complete task as efficiently as possible delegating to nodes that are better suited for travel to a given waypoint then others. This is handled by the task allocation algorithm.

Two algorithms, sharing a common root algorithm, are used. CBBA [10] does not support

clustered networks, and is used for the simulations in which nodes act as one large network. CF-CBBA [2] is used to demonstrate the benefits of clustering when considering network resource consumption.

Both algorithms have their communication protected by IPsec, VPLS, OpenVPN and SUPERMAN. The comparison of these protocols is intended to allow the analysis of the security service provision of each protocol, compared with their respective security overheads (the number of bytes transmitted during task allocation, including security).

Analysis of the network resource requirements of secure task allocation will allow an evaluation of the suitability of VPN and VCN approaches. This evaluation will specifically address suitability of either approach in the context of autonomous mobile ad hoc networks.

6. Results

Results are broken down into three types; network authentication, secure tunnelling and secure task allocation. These are further broken down into the number of communication events and the number of bytes transmitted. A sub-section analysing and discussing the security dimensions addressed by the VPN and VCN approaches that have been simulated, provides routing and security service analysis. This comparison is intended to identify the desirable features possessed by the VPN and VCN approaches to MANET security.

6.1. Network Authentication

Figure 3 shows the number of communication events required by SUPERMAN and VPLS during authentication with the network.

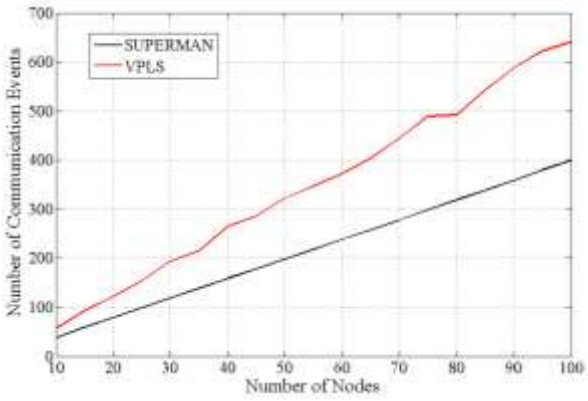

Figure 3. Graph showing the number of communication events required to authenticate all nodes with the network

VPLS is shown to consistently require more communication events to achieve network authentication than SUPERMAN. VPLS requires a central server for authentication with the mesh-like VLAN environment it creates for all member nodes, creating a central point of failure for the authentication of new nodes. This can also result in long routes between nodes and the central server node, unless the MANET maintains a dense topology.

SUPERMAN, only requiring that the neighbouring node (any node in range) is an authentic SUPERMAN node, with the appropriate certificate and protocol suite to facilitate network authentication, is more efficient in terms of communication events. In networks of 100 nodes, SUPERMAN requires 38% less communication events than VPLS.

Figure 4, however, demonstrates that the SUPERMAN requirement that certificates are exchanged bi-directionally and that neighbouring nodes perform security association alongside network authentication leads to much higher data requirements, despite fewer transmissions.

VPLS requires that the central authentication server provides a certificate to nodes able to authenticate with it via a puzzle-solution exchange mechanism. Successful authentication results in a certificate being exchanged with the petitioning node by the authentication server. Once authenticated, the node becomes a member of the VPLS mesh-Ethernet broadcast domain governed by the server.

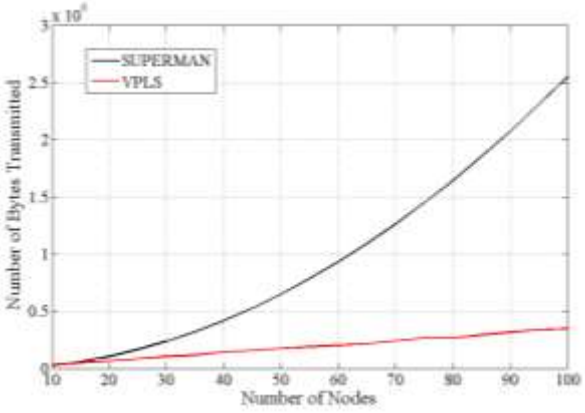

Figure 4. Graph showing the number of bytes transmitted when authenticating all nodes with the network

The completion of the authentication process results in the petitioning node possessing a Diffie-Hellman derived key for the VPLS domain to which it has subscribed, and a certificate as proof of its validity (provided by the authentication server).

SUPERMAN is shown to initially require less data than VPLS to authenticate with the network, but rapidly grows in cost as the network increases in size. This is due to the incorporation of identifying information and a *key share* in discovery packets, driving up the cost of probing for potential authenticator nodes.

VPLS requires 15.8% of the data needed by SUPERMAN, as connections with the central

authenticator node are established using a lightweight exchange of puzzle and solution data, the exchange of which is initiated by simple HELLO messages and terminated by a signed acknowledgement. The initialisation and termination messages are substantially smaller than those used by SUPERMAN, as point-to-point security is not applied. Diffie-Hellman key data is only exchanged once a connection has been established with the authentication server, reducing the size of HELLO packets considerable, when compared to SUPERMAN equivalents.

However, this process is entirely dependent on the central node being reachable. VPLS does not participate in, or secure, routing. As a result, the intermediate nodes involved in the communication of credentials between the authentication server and petitioning nodes cannot be considered as trustworthy. Any loss of contact or destruction of the central node will result in the authentication process failing and the node being unable to join the network.

SUPERMAN is resilient against such disruption, as it only requires that two nodes sharing a common-trusted-source (the certificate issuer or a higher authority shared by their issuers) to communicate and form a new SUPERMAN network. The additional cost is high, but required in networks with unpredictable topology and communication medium, such as MANETs.

VPLS will establish a VPN at a low initial cost, but only assuming that loss rates are low and that the central node remains reachable at all times. SUPERMAN, operating in a pre-route MANET (in which no routes have been formed), will incur a higher cost due to the larger packets and one-hop topology of the network during the authentication process leading to a more communication-intensive authentication process. SUPERMAN will, however, provide security to routing among nodes that have authenticated with the network and point-to-point security, whereas VPLS will not provide any security to routing among networked nodes and does not secure packets point-to-point.

6.2. Secure Tunneling

Figure 5 shows that SUPERMAN requires the least communication events to have all nodes form security associations (secure tunnels) between all other network members. IPsec requires the most by a considerable margin, while VPLS and OpenVPN, sharing a tunnel forwarding mechanism, have consistently similar communication event counts.

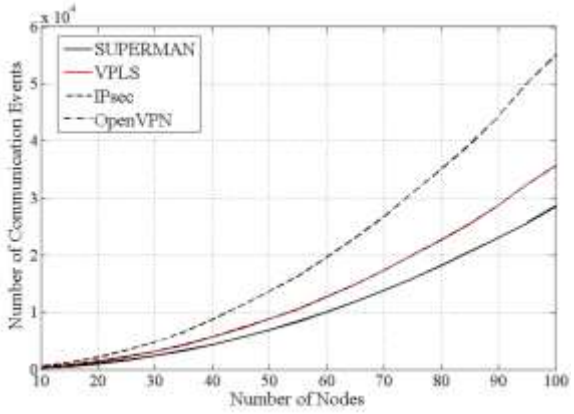

Figure 5. Graph showing the number of communication events that occur during the formation of secure tunnels between all nodes

SUPERMAN makes significant gains when forming secure tunnels between nodes. A delegated authentication mechanism allows SUPERMAN nodes to vouch for nodes that they know to be legitimate if they are on the route between source and destination when a source node attempts to form a secure tunnel with the destination node. This is possible due to the topology-aware characteristics of VCNs. When a MANET of 100 nodes is attempting to form secure tunnels between all member nodes, delegated authentication results in SUPERMAN requiring 19.5% less communication than VPLS and OpenVPN, and 46.3% less than IPsec.

Figure 6 shows that SUPERMAN, in networks of up to 47 nodes, requires the least data transmission to form secure tunnels. In larger networks, VPLS shows considerable scalability. IPsec is demonstrably the most expensive approach in terms of data utilisation for large networks, though in smaller network (60 nodes or fewer) OpenVPN is costlier in terms of data.

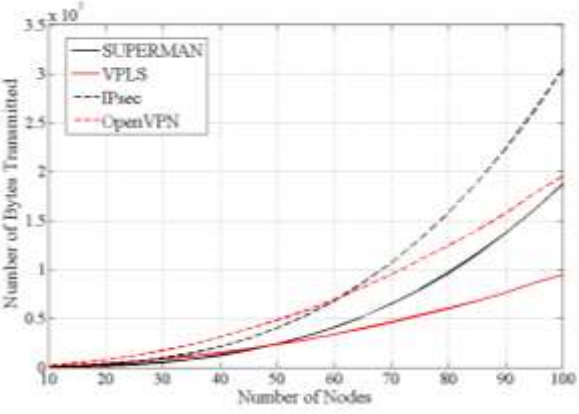

Figure 6. Graph showing the number of bytes transmitted when establishing secure tunnels between nodes

VPLS requires 45% less data to be transmitted to secure all nodes in the network, when compared with SUPERMAN in 100 node MANETs. This is due to the broadcast mesh-Ethernet approach taken by VPLS. Nodes do not require complicated key

exchanges, the central server determines send and receive keys ahead of tunnel formation, requiring that nodes only have to exchange identifying information and a *puzzle* variable to associate with each other. SUPERMAN requires the change of *key shares* to allow Diffie-Hellman key generation to occur and provide a unique key associated with the end-to-end and point-to-point links between source and destination.

SUPERMAN does benefit from the delegate authentication mechanism, which reduces the effective length of routes by allowing intermediate nodes already associated with the destination of a request for secure association to intervene and prevent further propagation of the request as it services the source-request for destination-credentials. As a result, SUPERMAN requires 9.2% less data than OpenVPN, and 41% less data than IPsec in a 100 node network.

Compared with VPLS, SUPERMAN offers point-to-point authentication and secure routing. VPLS offers neither of these services. As a result, SUPERMAN requires larger packets, but this provides extended and vital security services to the network.

6.3. Secure Task Allocation

Establishing a secure network is only one part of the VPN and VCN function. Providing secure communication to applications that require it is an ongoing service and can be considered the most important measure. As the comparison has been performed on the same allocation process in each iteration, the data is uniform aside from the addition of security overhead.

Figures 7 and 8 show the cost of performing CBBA task allocation, but it is important to note that the spikes and troughs in the data are driven by the underlying behaviour of the task allocation protocol. CBBA, more so than CF-CBBA, varies in the amount of allocation rounds required before reaching convergence. This number is affected by the number of nodes, their position respective to the task distribution in the simulation space and number of tasks. This occurs in such a way that it may be less computationally intensive to compute 45 tasks than it is to compute 40.

Figure 7 provides the results of CBBA simulation, using IPsec, VPLS, OpenVPN (OVPN) and SUPERMAN to secure the task allocation process.

IPsec is the most expensive of the four protocols, requiring 32% more bytes than SUPERMAN to provide security to a 50 task CBBA process. VPLS is second most expensive, by a thin margin, requiring 30% more network resources than SUPERMAN.

OpenVPN is a significant improvement over IPsec and VPLS in terms of security overhead. It requires 19.6% more data than SUPERMAN.

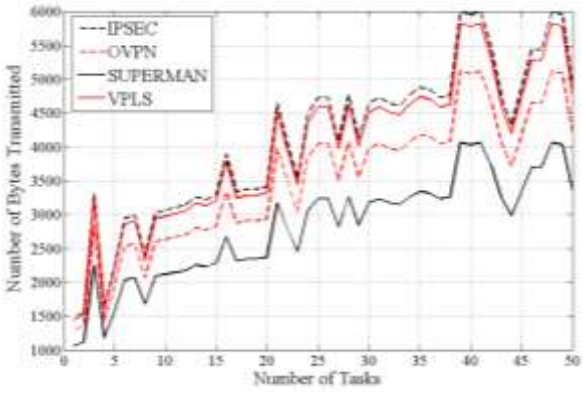

Figure 7. Graph showing the number of bytes transmitted when performing CBBA on 18 nodes

The primary contributing factor to SUPERMAN's apparent efficiency is the avoidance of data duplication, SUPERMAN does not require the encapsulation of whole data packets. It appends SUPERMAN security data to the data itself, before adding the IP header. This avoids duplication of the IP header.

Figure 8 shows the results of a CF-CBBA simulation using 3 clusters of 6 nodes. The data overhead of task allocation is significantly lower than that of CBBA, due to the partitioning of the number of tasks and processing between multiple clusters. This effectively allows the problem to be processed in parallel, reducing the amount of communication required.

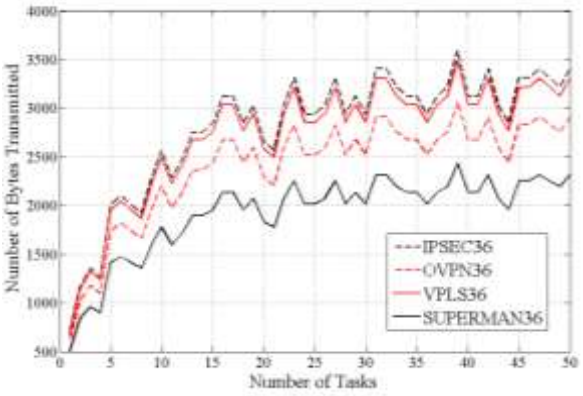

Figure 8. Graph showing the number of bytes transmitted when performing CF-CBBA in 3 clusters of 6 nodes

The trend observed in Figure 8 persists in Figure 9. For 50 task problems, IPsec requires 30.6% more data than SUPERMAN. VPLS requires 28.5% more data, and OpenVPN needs an additional 18.8% of data when compared against SUPERMAN in 50 task problems.

Figure 9 presents the results of simulation for a CF-CBBA process involving 3 clusters of 6 nodes. This is presented in addition to the results shown in Figure 9 as the organisation of nodes into clusters has an effect on the communication requirements of the task allocation process. This configuration is

costlier than the 3 cluster scenario used in Figure 9, but provides results with higher optimality when considering how nodes will execute allocated tasks [2].

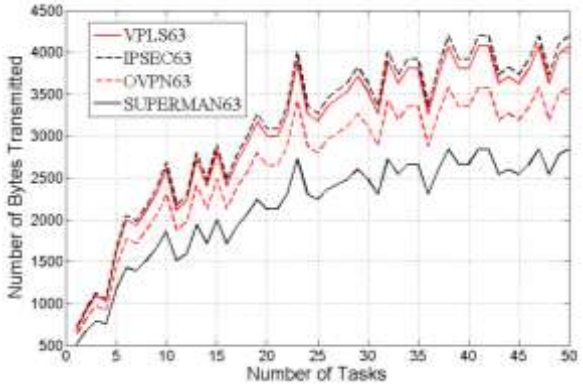

Figure 9. Graph showing the number of bytes transmitted when performing CF-CBBA in 6 clusters of 3 nodes

The results observed here have much in common with Figures 7 and 8. IPsec requires 32.3% more data than SUPERMAN for 50 task problems. VPLS requires 30.2% more data. Compared with SUPERMAN, OpenVPN requires 20.7% more data.

These results show that the security overhead of SUPERMAN is consistently lower than that of IPsec, VPLS and OpenVPN. Furthermore, it is shown that the configuration of nodes within the network, and the choice of task allocation protocol has no effect on the security overhead of VPN and VCN protocols, as evidenced by the similarity of security overhead comparisons in all three experiments.

In each experiment, IPsec is shown to have the highest cost, in terms of additional bytes required to secure communication. This is unsurprising, considering its focus on infrastructural, wireline networks that can rely on a robust and reliable communication medium.

VPLS is the second costliest, in each case. Like IPsec, it must encapsulate the data packet in a security packet, leading to address duplication. Unlike IPsec, VPLS does not require exhaustive configuration data in its header, instead requiring only the addition of MPLS data if operating in a MANET or telecommunications network configuration, and a 4 byte VPLS network identifier.

OpenVPN reduces overhead further, by avoiding the use of configuration data entirely. OpenVPN assumes that any member node will be knowledgeable about the configuration of the target VPN after it has joined.

It is the role of the VPN server to update any configuration data required by member nodes. Although this limits the flexibility and dynamism of OpenVPN, especially in a MANET scenario, it does result in a relatively small header for a VPN service.

As the VCN approach does not require duplication of data in the header, all SUPERMAN packets have comparatively low security overheads.

6.4. Provision of Security Services

ITU-T Rec X.805, as previously discussed, outlines eight security dimensions. These must be addressed at least in part to provide a secure environment for communication over any network.

Table 4 outlines the security dimensions provided by SUPERMAN, VPLS, OpenVPN and IPsec. SUPERMAN extends all eight security dimensions, providing access control by closing the network against any outside use or interference. Only nodes authenticated with the network may use network resources. Furthermore, adherence to the VCNs security protocols provides non-repudiation and communication security, which VPN approaches cannot guarantee.

The three VPN approaches do not provide access control, non-repudiation or communication security. None of the three analysed frameworks provide access control. VPLS controls access to the mesh-Ethernet domain it establishes, but nodes may still be routed over, unless segregated from the untrusted infrastructure over-which it may be communicating.

The VPNs analysed do not provide non-repudiation, as connections are usually end-to-end. Higher-authorities are involved in the authentication of nodes and provision of credentials to secure tunnels. This means that once a node has been given appropriate credentials, it is possible for that node to deny malicious action, unless trust-based systems are put in place to augment the baseline security provided by the VPN. Some implementations of IPsec and VPLS allow for unique timestamping to add an additional layer of identification to packets, providing a measure of non-repudiation by tying specific packets to identities in an irrefutable manner.

Table 4. The ITU-T Rec X.805 Security Dimension coverage of SUPERMAN (SMAN), VPLS, OpenVPN and IPsec

Security Dimension	SMAN	VPLS	OpenVPN	IPsec
Access Control	X			
Auth.	X	X	X	X
Non-repudiation	X			
Data Confidence	X	X	X	X
Comm. Security	X			
Data Integrity	X	X	X	X
Availability	X	X	X	X
Privacy	X	X	X	X

Communication security requires that information flows only between authorised end-points. Due to the tolerance of untrusted infrastructure by VPN approaches this cannot be guaranteed. Though it may be argued that the open-medium problem of wireless communication would compromise SUPERMAN's provision of such services, SUPERMAN does not allow routing over untrusted nodes. It therefore does not compromise communication security as a function of the framework itself, though it cannot entirely mitigate the open-medium problem.

By closing the network, using a VCN philosophy to prevent the use of untrusted routes, one can protect a MANET against trivial insertion of hostile nodes, identity theft and the destruction or dissemination of data by intermediate untrusted nodes on routes between end-points. SUPERMAN's additional cost is reflective of greater security service provision, and a more granular approach to network security in highly mobile, dynamic MANETs.

7. Conclusion

When comparing VPN and VCN approaches, it is important to bear in mind the target network. VPNs typically provide end-to-end security over untrusted infrastructure (with no security guarantees regarding the route taken between end-points), while VCNs secure a specific network by locking it down completely and not allowing propagation of data over untrusted parties to form a part of operational principle.

SUPERMAN, the VCN approach used as an example in this paper, also protects routing, and forms a secure network environment prior to routing operations. VPN approaches require that infrastructure is pre-existing, and that infrastructure may not be trustworthy.

Indeed, VPNs are intended to function over untrusted infrastructure, but for distributed MANETs of many nodes, this may not be feasible due to the relative intelligence of MANET nodes over static infrastructure. Untrusted nodes in a MANET scenario have far greater power to destroy or reroute data than mono-task switches and routers in conventional infrastructural networks, making them a significant threat to quality of service and network resources.

VPN approaches to secure MANETs have been recorded in a considerable body of scientific literature, including attempts to use IPsec, OpenVPN and VPLS to allow secure communication between MANET nodes in wireless sensor, micro-UAV and UAV swarm scenarios. Each approach tends to treat other MANET nodes as untrusted, ignoring the potential offered by the topology-awareness and control of MANET nodes. VPN approaches fail to account for a variety of attacks that MANETs are extremely vulnerable to, for example, man-in-the-middle, impersonation and Sybil attacks. They are also vulnerable to attacks that abuse route-agnostic systems, such as black hole and wormhole attacks.

A VCN ensures that only authenticated members of the network are included on secure communication routes, mitigating the issues caused by route-agnostic communication being abused by malicious undetected intermediate nodes. The proposed framework extends cost-saving measures, as MANETs have a potentially unreliable communication medium, resource-constrained network hardware, in many cases.

Simulation of SUPERMAN and three VPN approaches has shown that SUPERMAN performs favourably when considering the number of transmissions required to authenticate all nodes with the network and form secure tunnels between all nodes. However, VPLS has been shown, in 100% reliable communication conditions, to require less data due to its lightweight, low-complexity approach to constructing a virtual mesh-Ethernet domain for its member nodes. As discussed in sub-section 6.3, the inclusion of untrusted nodes in the routing process, and the lack of route-security under VPLS, compromises any expectations of 100% delivery rates. VPLS does not address the core issues of route-agnosticism leading to an inability to diagnose and cope with rerouting, destruction and manipulation of data between nodes. It also is not designed with unreliable transport as a consideration, requiring a reliable (if untrusted) infrastructure to facilitate communication between nodes.

Simulation of SUPERMAN, IPsec, VPLS and OpenVPN in the context of providing security for application communication, showed that SUPERMAN is more efficient than its VPN peers. This is due to the integration of SUPERMAN into the network stack itself, it operates as an integral part of the flow of data from the application layer through the network layer. As a result, it does not need to encapsulate data packets, and avoids the additional cost of IP and TCP/UDP data duplication. This makes it a suitable candidate for security in resource constrained networks that afford nodes a high level of individual control over the network. MANETs, especially autonomous ones, are a good example of such a network.

In highly mobile MANETs with potentially unreliable wireless communication, packet loss may be considerable. This would have a highly adverse effect on VPLS, as it requires periodic communication with a central node on the part of all member nodes to ensure all keys are up to date for secure communication. As a result, it may be concluded that expecting 100% delivery rates in a MANET is ill-advised, even before considering the inherent unreliability of wireless communication. It is trivial for malicious nodes to place themselves on a route, and sink or disseminate data, as VPLS does

not provide any protection other than integrity and confidentiality to data in transit, and is unaware of the route taken.

Future work will focus on mobile nodes with variable reliability to further analyse the effectiveness and efficiency of VPN and VCN approaches to secure MANET communication. Of particular interest is the effect that increasing loss rates will have on VPLS, as it has performed very well in terms of efficient communication for scenarios assuming perfect communication characteristics. Side-by-side comparison of SUPERMAN and VPLS will be a focal point in the research undertaken to analyse the effect of mobility and unreliable communication on secure MANET formation; and how such negative impacts on performance can be reduced.

In addition, an implementation of SUPERMAN as a Linux kernel module and daemon is under development and a real-world comparison of SUPERMAN and VPLS will be considered as well as the release of SUPERMAN under an open source software licence.

8. References

[1] J. Page, T. Chi, D. O'Neil et al., "Self-organised swarms; a technology for aerospace," 2015.

[2] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A cluster-based approach to consensus based distributed task allocation," in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.

[3] N. Doraswamy and D. Harkins, IPsec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003.

[4] X.-c. GUO and Z.-j. ZHAI, "Investigation on security of openvpn architecture [j]," Science Technology and Engineering, vol. 8, p. 056, 2007.

[5] M. Lasserre and V. Kompella, "Virtual private lan service (vpls) using label distribution protocol (ldp) signaling," Tech. Rep., 2007.

[6] B. Ballav and G. Rana, "A review of routing attacks in manet and wsn," in International Journal of Engineering Development and Research, vol. 3, no. 2 (May 2015). IJEDR, 2015.

[7] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," Security and Communication Networks, vol. 6, no. 4, pp. 523–538, 2013.

[8] P. Gupta and K. Gauri, "Solution of cooperative black hole attack problem in mobile ad-hoc network," International Journal of Advanced Research in Computer Science, vol. 3, no. 2, 2012.

[9] J. Loo and M. Aiash, "Challenges and solutions for secure information centric networks: A case study of the netinf architecture," Journal of Network and Computer Applications, vol. 50, pp. 64–72, 2015.

[10] Choi, H.L., Brunet, L. and How, J.P., 2009. Consensus-based decentralized auctions for robust task allocation. Robotics, IEEE Transactions on, 25(4), pp.912-926.

[11] E. N. A. Hamdi and I. H. A. Hussaini, "Point-to-point virtual private network based on ip filtering and rijndael encryption algorithm," Network and Complex Systems, vol. 4, no. 7, pp. 1–9, 2014.

[12] M. Feilner and N. Graf, Beginning Open VPN 2. 0. 9: Build and Integrate Virtual Private Networks Using OpenVPN. Packt Publishing Ltd, 2009.

[13] W. Dong and Z. Y. Zhang, "Research on virtual private lan service signaling protocol and its application," in Applied Mechanics and Materials, vol. 543. Trans Tech Publ, 2014, pp. 2585–2588.

[14] M. Liyanage and A. Gurtov, "Securing virtual private lan service by efficient key management," Security and Communication Networks, vol. 7, no. 1, pp. 1–13, 2014.

[15] S. M. R. Jafri, "Securing and optimizing the communication in mobile ad hoc network (manet)," International Journal of Technology and Research, vol. 2, no. 2, 2014.

[16] Smith, Darren P., Wetherall, Jodie and Adekunle, Andrew (2015) Virtual Closed Networks: A Secure Approach to Autonomous Mobile Ad hoc Networks. In: Internet Technology and Secured Transactions (ICITST-2015), The 10th International Conference for. IEEE, London, UK, pp. 391-398.

[17] Perkins, C., Belding-Royer, E. and Das, S., 2003. Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[18] E. W. Dijkstra, "A note on two problems in connexion with graphs," Numerische mathematik, vol. 1, no. 1, pp. 269–271, 1959.

[19] Choi, H.L., Brunet, L. and How, J.P., 2009. Consensus-based decentralized auctions for robust task allocation. Robotics, IEEE Transactions on, 25(4), pp.912-926.

