Virtual Private Broadband Access in Metropolitan-Area Wireless Mesh Networks

Xiaodong Lin, Pin-Han Ho, and Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering, University of Waterloo, Canada
{xdlin,pinhan,xshen}@bbcr.uwaterloo.ca

Abstract – *Virtual Private Network* (VPN) is one of the killer applications in the modern Internet carriers which support enterprise premium services with custom-designed control primitives and security assurance. By envisioning that *Wireless Mesh Networks* (WMNs) will be a complement to the state-of-the-art last-mile technologies in metropolitan areas, this paper introduces a novel framework of VPN design and implementation for service-oriented WMNs. In particular, the paper deals with the issues of network architecture design and secure user authentication. The introduced framework is characterized by high self-configurability, inter-operability, and compromise resilience in presence of malicious attacks and compromise events without losing the ability of supporting interactive and real-time services such as VoIP and video phone.

Index terms – Virtual Private Network, Wireless Mesh Network (WMN), IEEE 802.21, Handover, Security

I INTRODUCTION

The adoption of *Wireless Mesh Networks* (WMNs) for supporting service-oriented metropolitan-area applications has attracted explosive attentions from both industry and academia in the past a few years [1,2]. WMNs based on IEEE 802.11s is a promising complement to the legacy wired *Digital Subscriber Line* (DSL) and Cable Modem services due to its flexibility, reliability, ease of deployment, and cost efficiency. A WMN is mainly composed of a cloud of distributed *Mesh Points* (MPs) as the backhaul. Each MP can be connected possibly to all the other MPs in its transmission range, by which the network topology is formed. A data route with multiple hops could be created by performing *Media Access Control* (MAC)-layer forwarding for the launched traffic in each intermediate node. A routing table is maintained at each intermediate node to facilitate hop-by-hop forwarding, where the MAC address of the next hop for each data path traversing through the node is kept. A number of physically adjacent MPs are grouped to form an Extended Service Set (ESS) corresponding to an Internet gateway, which interfaces the ESS with the public Internet.

Different from mobile ad hoc networks (MANETs), the WMN infrastructure is expected to be public asset and operated by the city government or an authorized communication company. The WMN will be supporting numerous WISPs and enterprises which lease the access to the WMN and request to form *virtual private networks* (VPNs) for their registered users. Each VPN, thus, will have to support its customers and employees based on the pre-defined *service level agreement* (SLA).

Layer-2 VPN [3] in the wired Internet has been extensively studied in the past decade, and the associated application scenarios and emerging services have been sufficiently defined. However, to the best of our knowledge, the development of WMN backhaul with a VPN service support has not been addressed. The following three issues are identified with an utmost importance for realizing the application scenario due to its unique features and requirements. Firstly, with multiple air interfaces and MAC protocols coexisting in a single mobile station (MS), a suite of routing and signaling protocols that can coordinate the peer entities by performing multi-hop explicit path selection is necessary, and should be standardized as a shim layer in order to achieve ineroperability and platform-independency. The shim layer can also help to achieve the layer-2 VPN functionalities, such as dynamic self-configuration, tunneling encapsulation, private IP address assignment, and traffic engineering [3].

Secondly, since numerous independent leasing WISPs and enterprises could run their business on top of the WMN infrastructure and control plane, handover and roaming operations could be frequently triggered due to the small coverage of each MP, which will certainly result in significant overhead and handover delay in case there is no an efficient yet reliable user authentication mechanism. Thus, how to reduce the signaling overhead and authentication delay without losing security assurance in order to support those highly interactive real-time services will be critical to the success of the WMNs with a VPN service support.

Thirdly, since each MP is a low-cost device with less security and hardware protection, it could be easily compromised by the adversary, which may cause *Denial of Service* (DoS) or network resource abuse. In addition to the conventional authentication and secure routing schemes, a suite of interoperable intrusion detection and node revocation mechanisms along with strong compromise resilience and fault-tolerance facilities is more than essential. The whole system should be equipped with in-depth defense to any malicious intrusion for maintaining the network functionalities, even in the presence of multiple compromised MPs.

To address the abovementioned issues, the paper aims to create a new framework of virtual private broadband access in metropolitan-area WMNs. We propose a network architecture with a layer-2 VPN service support, where IEEE 802.21 [4] forming a shim layer between IP and vendor-specific MACs is adopted and extended for this application. Furthermore, we develop a secure framework

for achieving in-depth defense of improving recilience of user authentication functionalities to any MP compromise event without losing efficiency in supporting real-time services. To the best of our knowledge, this is the first paper discussing how to realize a VPN in a WMN environment.

The remainder of the paper is organized as follows. Section II gives a general introduction to the network architecture of interest. Section III describes the IEEE 802.21 standardization progress and the possible extensions which are essential for supporting the VPN services in heterogeneous WMNs. Section IV studies secure user authentication, where a novel compromise resilience architecture based on a (*t*, *n*) threshold authentication mechanism is introduced. Section V concludes this paper.

II NETWORK ARCHITECTURE

A *Architecture of VPN on WMNs*

The network entities in the WMNs of interest are illustrated in Fig. 1, where a general 4-tier network architecture is formed. The first layer is the *logic tier*, which is composed of numerous VPNs formed by all the independent WISPs and enterprises. Each VPN is also referred to as a *realm* (or a logic domain) defined with a group of MUs along with the corresponding QoS and security & privacy requirements. The second tier includes the *mesh clients*, which are also referred to as MSs possibly equipped with multiple MAC protocols and air interfaces. The *mesh clients* could be either single-user mobile devices such as laptops and handheld PDAs, etc., or wireless network bridges which interface the mesh clients with the wireless mesh backbone in the underlying layer.

The third layer has MPs forming a multi-hop WMN backhaul with multi-radio multi-channel wireless capabilities. From the control and management perspectives, two types of MPs are defined. One is *mesh access point* (MAP) which provides all the functionalities of a *mesh point* (MP), including the access by the *mesh clients* and the communication with the Internet gateways at the fourth layer. The others are the *light-weight mesh points* (LWMPs), which primarily serve as relays aiming to improve the network throughput and coverage. The fourth layer consists of the Internet gateways, which interface the WMN with the public wired Internet.

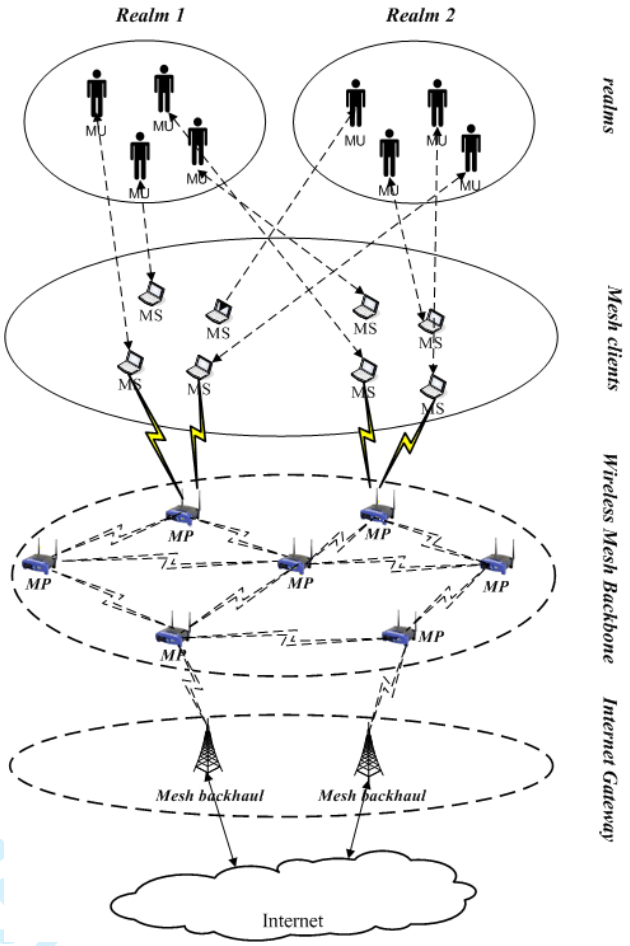


Fig. 1. A four-tier WMN-based VPN architecture.

B *Layer-2 Virtual Private Networks (VPNs) in WMNs*

The *Multi-Protocol Label Switching* (MPLS) based layer-2 VPN [4] has been well studied and practically launched in the conventional wired Internet. With MPLS, different layer-2 technologies (such as ATM, SONET, Frame Relay, Ethernet, etc.) can be accommodated under a single control plane without any awareness in the development of the upper layer (i.e., IP) software artifacts. The network carrier has its core network interconnected with the *Provider's Edges* (PEs), which are the edge nodes of the network. An enterprise or an ISP can lease the access to the provider's carrier through a set of PEs by allocating a *Customer Edge* (CE) connected to the PE of interest. Each CE serves as a control unit which stipulates everything in the *Service Level Agreement* (SLA) for the VPN, such as the QoS assurance, types of services supported, authority, and authentication methods, along with the custom-defined primitives, functionalities, and private IP addresses, etc. The associated IP compatible protocols, such as *Open Shortest Path First* (OSPF) and *Resource ReSerVation Protocol* (RSVP) with traffic engineering extensions, define how the routing, signaling, and resource reservation are performed.

When layer-2 VPNs are implemented on WMN backhaul, more complicated design and research issues must be addressed due to some of the unique features brought up in the new networking scenario, such as the high frequency of handover/roaming events, small coverage of each MAP, and new security threats due to the open medium access through the air. Under such a circumstance, it is far from scalable and cost-effective for a leasing WISP to install all the MAPs of interest with a hardware-based VPN CE. Instead, software-based signaling mechanisms and protocols must be developed in the MAP cloud in order to achieve light-weight configuration and autonomous coordination for the VPN service maintenance. The signaling mechanisms and protocols should support multi-hop routing under both tunnel and transport modes, localized user authentication, and physical layer parameter exchange among MAPs that can enable efficient and customized tunnel establishment specific to the corresponding SLA. Therefore, it is inevitable to tackle the problem of standardizing a layer-2 protocol that can achieve better interoperability and platform independency in the task of VPN setup and maintenance.

III VPN SUPPORT THROUGH IEEE 802.21

In the metropolitan-area WMN, integration of heterogeneous network domains is a trend leading to a ubiquitous and pervasive communication environment. A MS with multiple MAC protocols and air interfaces is expected to be *Always Best Connected* (ABC) to the corresponding node for the Internet access through one of the available air interfaces according to a cross-layer decision making process. This task can only be achieved through vendor-specific devices and software programs in case no standardized approach for performing event, information, and command services is available, which makes the VPN support in WMNs difficult.

To achieve inter-operability, the 802.21 working group has put extensive efforts on a standardization process for IEEE 802.x media access-independent mechanisms. The first draft on Media-Independent Handover Function (MIHF) has emerged in March 2006, and the third draft has quickly came up in December 2006 [4], which has successfully defined the service models along with a unified software/signaling framework for achieving seamless interworking and information exchange.

IEEE 802.21 helps with handover initiation, network selection and interface activation during handovers. In addition, IEEE 802.21 enables co-operative handover decision making between the clients and the network. With this, the network operation and management can optimize handovers between heterogeneous 802 systems (such as 802.3, 802.11, and 802.16) and between 802 systems and cellular systems (such as 3GPP with CDMA 2000) with intelligence and inter-operability.

The service model defined in 802.21 for the interworking of 802.11, 802.16 and cellular networks is illustrated in Fig. 2, where a shim layer performing MIHF between the IP (layer 3) and link layer (layer 2) is formed. The *media-independent handover service access point* (MIH-SAP) interfaces the MIHF with the higher layer entities, such as transport control, handover policy functions, and layer-3 mobility management primitives. Meanwhile, LLC-SAP and 3GLink-SAP are two media-dependent SAPs that allow the MIHF to use services from the lower layers of the mobility management protocol stack and their management planes. Since the link layer parameters and existing software artifacts could be very vendor-specific, the adoption of the MIHF serving as the 2.5 layer can greatly improve the system interoperability and facilitate the emergence of new services and applications.

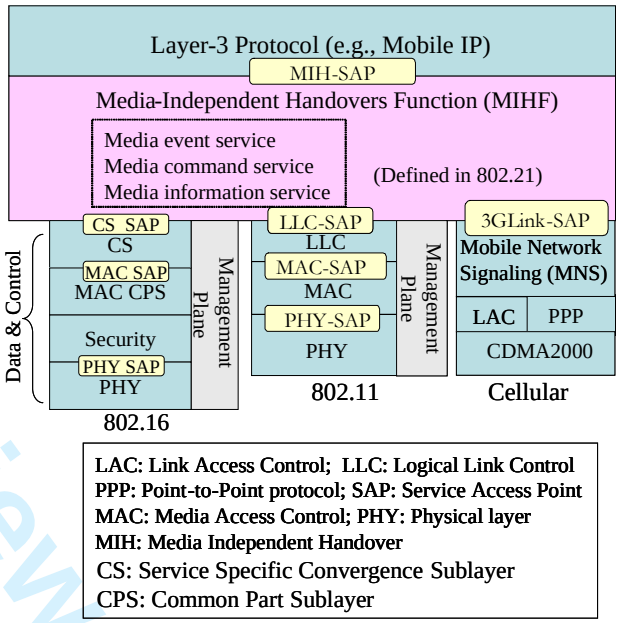


Fig. 2. The service model of IEEE 802.21 for supporting VPN services in WMNs with heterogeneous MAC protocols and air interfaces under IEEE 802.16, 802.11 and CDMA2000 cellular systems.

To equip a WMN with the VPN support, we extend the IEEE 802.21 standard to serve as a platform-independent inter-domain routing and signaling protocol with QoS and security functionalities. The extensions cover the following three aspects:

- **Media Independent Information Services (MIIS):** The IEEE 802.21 media information service deals with information exchange among 802.21 peers for neighborhood exploration. To support VPN services, multi-hop information services that support additional routing and signaling information exchange within the MP cloud should be defined on top of the original MIHF. For example, in addition to the event services designed for MIHF, some traffic engineering parameters for enabling multi-hop routing and resource allocation must defined, such as customized link metrics, availability of radio resources and maximum reservable capacity of a remote peer in the MP cloud. The labels for achieving class of services and data encapsulation are also critical, which concerns how the network can differentiate traffic

flows with different grades. In addition, to achieve auto-configuration for VPN validation at each MP, the information services should encompass the information that can support issuing remote instructions for VPN validation, *security association* (SA) establishment/release. More sophisticated operations, such as the support of cooperative user authentication, should be allowed for an easy and lightweight *Certificate Revocation List* (CRL) update in case any *Public Key Infrastructure* (PKI) based authentication framework is adopted.

- **Media Independent Command Services (MICS):** The command services aim to carry the MIHF or even upper layer decisions to the lower layers on local MS entity or at remote entity [4]. In general, the command agent in the MIHF should be equipped with command primitives for the corresponding services. For example, the command agent should issue a link command to the lower layer to notify the authentication decision, channel/bandwidth allocation decision, and communication mode selection (i.e., tunnel or transportation mode, etc.), such that the lower MAC layer can process the incoming/outgoing packets properly. Also, the command agent should be responsible for requesting the link status and possibly any physical layer parameter in order to facilitate radio resource management and traffic engineering functionalities.
- **Media Independent Event Services (MIES):** The IEEE 802.21 event services are the information flows initiated at the lower layers, which can be used to notify the upper IP layer any change in the state and transmission behavior of the underlying logic link, MAC, and physical layers, or predict state change of these layers. To enable integration of heterogeneous networks and form a unified service plane, the local MIES function should be extended to support any routing or link-layer scheduling mechanism for improving throughput and system capacity. For example, the MIES should proactively inform the MIHF the change of link state and summarized information on the queue status and traffic statistics so as to achieve efficient resource allocation, packet scheduling, and connection admission control. On the other hand, the remote MIES function should alliance the local and remote peers to form an autonomous system such that the information exchange can be performed efficiently. This is fundamental to achieve an intelligent and self-configurable network environment that is required by a low-cost and high-fidelity layer-2 VPN on WMNs.

In summary, it is critical to have a suite of standard mechanisms and SAPs dedicated for supporting VPN services in metropolitan-area WMNs in order to achieve interoperability and media-independent auto-configuration. This is particularly essential when the numbers of MPs and WISPs/enterprises are getting larger with more diversified technologies coexisting in the entire network domain.

IV SECURE USER AUTHENTICATION

User authentication is another essential and unique issue in the WMNs of VPN service support. Due to a small coverage of each MAP and the stringent demand for many emerging online multimedia services such as VoIP, the events of user handover and roaming along with authentication requests are expected to appear much more frequently with a stringent delay requirement compared with that in the conventional cellular networks. In particular when VPN services are supported, a secure and localized user authentication mechanism is required not only for the avoidance of illegitimate accesses of network resources, but also for the enterprise security and user privacy that are intrinsic to the success of VPN services.

A Security and Compromise Resilience with AAA Framework

Currently, the best practice of ensuring security in wireless networks is by way of the *authentication, authorization and accounting* (AAA) framework, where an AAA server is adopted to perform authentication, authorization, and collect accounting data for each user requesting for the Internet access [5]. Fig. 3 shows the AAA framework based on 802.1x with the *Extensible Authentication Protocol* (EAP) [6]. When a MS enters the radiation range of an *access point* (AP) and tries to associate with the AP, the AP inspects the MS's association and enables the MS's wireless connection. The MS then sends an *EAP-Start* message.

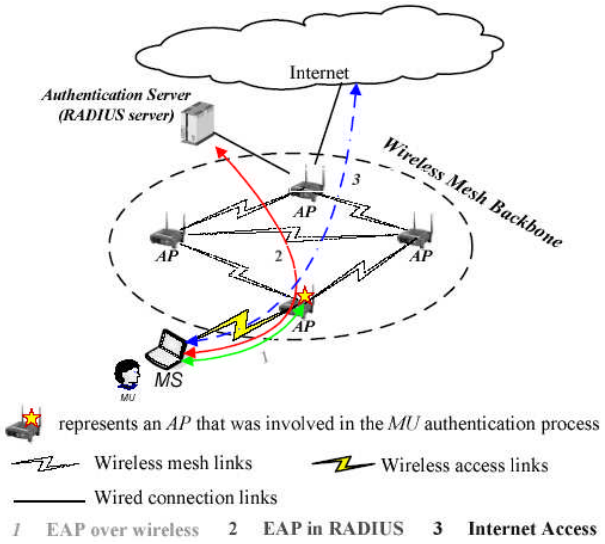


Fig. 3. Authentication process with 802.1x in wireless mesh networks.

The AP replies with an *EAP-Request Identity* message back to the MS to obtain the MS's identity. The MS's *EAP-Response* packet containing the MS's identity is then forwarded to the AAA server. Afterwards, the AAA server, e.g. RADIUS server, issues a *RADIUS Access-Challenge* to the AP. After receiving the Radius Access-Challenge, the AP issues an authentication challenge to the MS, which is supposed to respond the challenge with its credentials. Then

the AP forwards the user authentication credentials to the authentication server. At the end, an *ACCEPT* or *REJECT* notification is sent from the AAA server to the AP. If an *ACCEPT* is received, the AP transitions the MS's wireless network connection to an authorized state. Finally, the MS has the network access. Once the authentication is complete, a key agreement process is invoked such that the MS and AP possess the corresponding secret key at the end of procedure, respectively, where the confidentiality and integrity of communication between the MS and the AP are protected by the session key.

Based on the AAA framework, several user authentication schemes have been proposed. Lamport [7] proposed the first well-known password authentication scheme based on a password table for achieving user authentication. Hwang and Li [8] presented an ID-based user authentication scheme by taking advantage of smart cards, although the passwords in their scheme were not low-entropy. More studies and related research on user authentication schemes have been reported afterwards [9].

However, since the previously reported user authentication schemes were developed virtually over a single authentication server, they may suffer from two types of failures in terms of the authentication functionality. The first type of failure occurs due to physical/protocol faults or a *Denial-of-service* (DoS) attack caused by any misuse, misconfiguration, and malicious access, which can simply make the server unavailable. In this case, the network becomes unavailable for performing authentication, which leads to revenue loss and service disruption. The impairment due to this type of failures can be well mitigated by allocating multiple redundant authentication servers working in a manner of distributed Duplicated Database (DB) such that the unavailability of one or a subset of servers will not affect the whole network authentication operation. In this way, the availability of authentication functionality in the network (or termed *authenticability*) can be significantly improved in the presence of any physical/protocol failure and DoS attack.

The other type of failure is due to an authentication server compromise event by one or a group of malicious attackers, which may cause even more serious damages and, unfortunately, cannot be solved by equipping the network with multiple independent and identical authentication servers. Such a network status is termed *false-authenticative*, which is one of the worst situations that the network defense system could be subject to. The problem lies in the fact that the false-authenticative status occurs as long as any one of the authentication servers is compromised, where the attacker can manipulate the compromised server and launch various vital attacks to the network operations such as allowing unauthorized network access, etc.

In order to further guarantee the system security and authenticability, the user authentication architecture should be developed such that the system can survive from the situation where one or a subset of authentication servers are compromised by a malicious intruder. The characteristic of intrusion tolerance is expected to be critically demanded in the future WMN design, which can assure the VPN services with better survivability in presence of malicious attackers.

One of the approaches for improving the compromise resilience is by way of a (t, n) threshold authentication mechanism, such that t or more than t out of n authentication servers can grant the access request of a MU, while t – 1 or less cannot. A generic (t, n) threshold authentication system based on the AAA framework is illustrated in Fig. 4, where the threshold cryptography [10] is implemented.

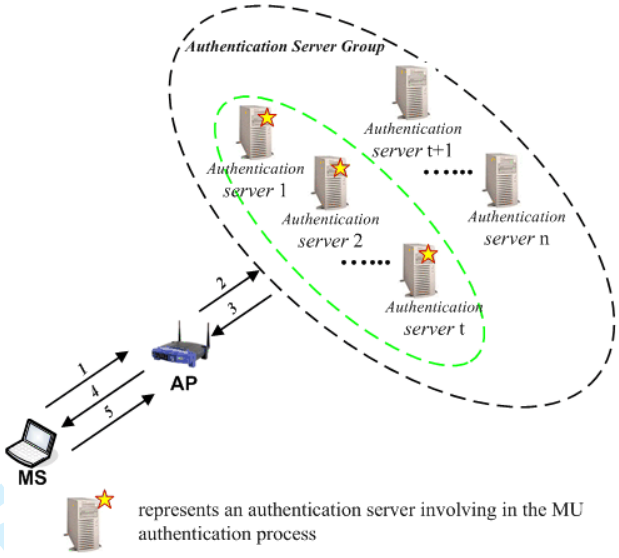


Fig. 4. A (t, n) threshold user authentication system on top of the legacy AAA framework.

B Compromise Resilience with Localized Authentication

Since there could be hundreds of MAPs deployed with thousands of MUs, taking the conventional centralized AAA framework for performing user authentication would potentially suffer from a serious scalability problem. Meanwhile, the AAA framework would certainly induce a significant amount of latency in the authentication process because of the propagation and possible queuing delay in the AAA server(s). The long authentication delay could be intolerable in the handoff process of some highly interactive real-time services such as VoIP. Thus, *localized authentication* [11] has been proposed to overcome the disadvantages in the employment the AAA server architecture, and is envisioned to serve as one of the major enabling technologies in the metropolitan-area WMN supporting VPN services.

One of the implementation difficulties in realizing localized authentication is on the dynamic signaling exchange and CRL update in the WMNs, which relies on a sophisticated and reliable standard signaling protocol. With the support of 802.21 signaling mechanisms extended from the MIIS, such a task could be easily addressed, where user credentials and cryptographic tips for enabling localized authentication could be exchanged through the shim layer with the minimum efforts in revising the current IP layer software artifacts. In this case, a WISP can customize and differentiate the security requirements of each class of service with an interoperable and standardized approach.

The localized authentication, however, is subject to a new problem in the effort of security assurance. Since localized authentication has each MAP equipped with more authorities and a larger database, a much more serious impairment will be induced when a MAP is compromised by a malicious attacker, which may lead to disruption of the legitimate network functions/services. Nonetheless, it may take much more investment in improving each MAP in terms of its protection and security devices in WMN, which obviously countermeasures the original design premise for achieving an economical and light-weight wireless backhaul.

Similar to the case of AAA framework, the network compromise resilience in the WMN with localized authentication can also be improved using the (t, n) threshold authentication mechanism, where n is the number of authenticators in an authentication group (AG), while t is the threshold on the number of authenticators of approval. Fig. 5 illustrates an event of (3, 7) threshold authentication, where the authentication of the MS is through an AG with 7 MAPs. The MU can be granted with the Internet access if 3 or more than 3 MAPs' contribute their partial signatures, by which the MU will receive a feasible session key for initiating the Internet access.

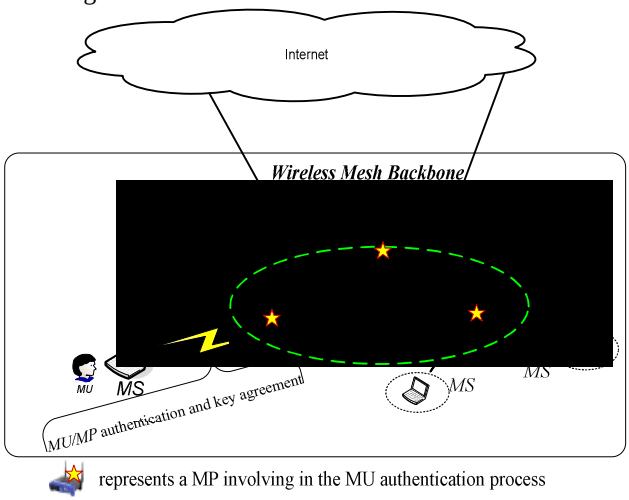


Fig. 5. An illustration on the MP compromise resilience architecture using a (3, 7) threshold authentication mechanism.

C Evaluation of Authenticability

The (t, n) threshold authentication mechanism is expected to achieve high authenticability. This section aims to verify the mechanism by conducting a comprehensive evaluation on the user authenticability in a number of case studies, by which the parameters t and n are determined.

Let each authenticator be possibly subject to two types of failures: one is the *compromise failure* due to a malicious attack with a probability v, and the other is the *DoS failure* with a probability of u. Note that a compromised failure is defined as a compromise event on an authenticator such that the attacker can launch various attacks on the whole network; while a DoS failure could be due to not only hardware/protocol problems, but also any malicious DoS attack that makes the authenticator unavailable for performing authentication function. We are interested in deriving the user authenticability under the (t, n) threshold authentication mechanism.

Let a failure event hit each authenticator independently. Let U and V be two random variables representing the number of authenticators that are subject to a compromise failure and a hardware/protocol failure at a specific time moment, respectively. Three states in terms of whether the network can well perform the authentication functionality are defined as follows: (i) authenticative, (ii) unauthenticative, (iii) false-authenticative. The first state happens when the total number of unavailable authenticators and compromised authenticators is less than or equal to $n - t$ such that at least t authenticators can authenticate a legitimate user login request. Besides, the number of compromised authenticators must be less than t such that there is no chance for the event of false-authenticative to occur. Thus, we have Eq. (1) to describes the first state.

$$\begin{cases} U+V \le n-t \\ U < t \end{cases} \quad (1)$$

The second state happens when the number of unavailable and compromised authenticators is larger than or equal to $n - t - 1$ such that there are not sufficient available authenticators to authenticate a legitimate user. We have Eq. (2) to describe the second state:

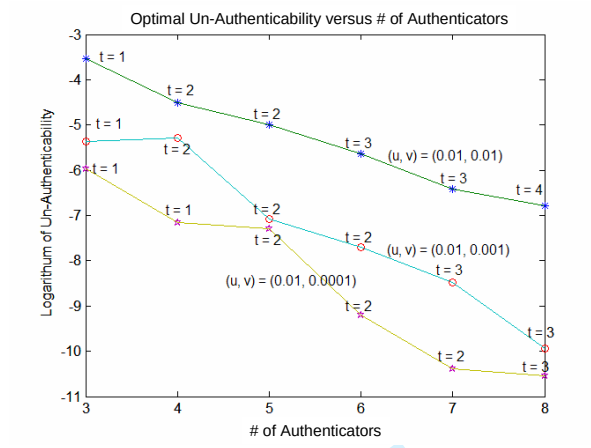
$$\begin{cases} U+V \ge n-t-1 \\ U < t \end{cases} \quad (2)$$

The last state occurs when at least t nodes among the AG of n are compromised, i.e.,

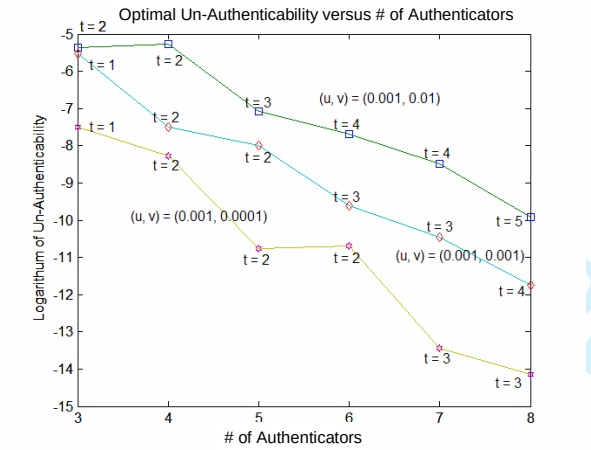
$$U \ge t \quad (3)$$

By assuming that U and V follow the binomial distribution with parameter u and v, respectively, we can derive the user authenticability, denoted as $\Pr\{U+V \le n-t, U < t\}$, based on Eq. (1). Obviously, the user authenticability is determined by t and n, where the value of t is bounded by n. Also, with more authenticators in an AG (or with a larger n), the user authenticability can be further improved.

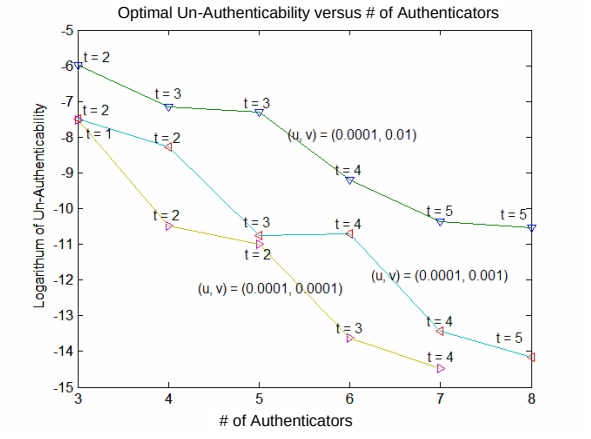
We simulated different combinations of u, v, t, and n. The values of 0.01, 0.001, and 0.0001 for u and v are tested, while the values of 4 to 8 for n are tested. The results are shown in Figs. 6(a), 6(b), and 6(c), respectively.



(a)



(b)



(c)

Fig. 6. The logarithm of the optimal network un-authenticability versus the number of authenticators in an AG with different combinations of u and v, where the threshold for the best authenticability is shown beside the data.

It can be seen that the (t, n) threshold authentication mechanism can achieve a significant improvement against the conventional authentication architecture in terms of authenticability. Note that with the conventional authentication, the un-authenticability is in the same order as u and v. It is also verified that n does not need to be very large to achieve high network authenticability. Therefore, we can simply select the one-hop or two-hop neighbors of a MAP to perform the threshold authentication for the MAP, where the partial signature can be generated by each authenticator in parallel in order to reduce the propagation delay in the authentication process. From our analysis, the authenticability can be as high as "10 nines" with (u, v) = (0.001, 0.001), where (n, t) = (3, 7).

V CONCLUSIONS

In this article, we have identified and characterized a framework of new application scenario on metropolitan-area wireless mesh networks (WMNs) to support virtual private broadband access. The proposed framework is expected to serve as an essential guideline in achieving a VPN service support in WMNs with heterogeneous communication technologies. Furthermore, we have defined and evaluated the user authenticability by jointly considering failures due to compromise events and DoS events, which is expected to create a new paradigm of design and development for user authentication schemes in WMN backhaul with compromise-prone MPs.

REFERENCES

[1] J. Eriksson, S. Agarwal, P. Bahl, and J. Padhye, "Feasibility Study of Mesh Networks for All-Wireless Offices", ACM/USENIX MobiSys, Upsalla, Sweden, June 2006.

[2] I. F. Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks", *IEEE Communications Magazine*, Vol. 43, No. 9, Sept. 2005, pp. 23 – 30

[3] W. Luo, C. Pignataro, A. Y. H. Chan, and D. Bokotey, Layer – 2 VPN Architecture, 2005, CISCO press.

[4] *Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services: IEEE P802.21/D03.00*, Std., Dec. 2006.

[5] C. De Laat, G. Gross, and L. Gommans, "Generic AAA Architecture," RFC 2903, March 2000.

[6] B. Aboba, *et. al.* "Extensible Authentication Protocol (EAP)", RFC 3748, June, 2004.

[7] L. Lamport, "Password Authentication with Insecure Communication," *Communication of ACM*, 24 (11), pp. 770 - 772, 1981.

[8] M. S. Hwang, and L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Trans. Consum. Electron.* 46 (1), pp. 28 - 30, 2000.

[9] R. Lu, and Z. Cao, "Efficient Remote User Authentication Scheme Using Smart Card," *Computer Networks*, 49 (4), pp. 535 - 540, 2005.

[10] Y. Desmedt and Y. Frankel, "Shared generation of authentication and signatures," In *Advances in Cryptology - CRYPTO'91*, Springer-Verlag, Berlin, pp. 457-469, 1991.

[11] M. Long, C. -H. Wu, and J. D. Irwin, "Localized authentication for inter-network roaming across wireless LANs," *IEE Proceedings Communications*, vol. 151, no.5, pp. 496-500, Oct. 2004.