Computer Networks 66 (2014) 94–101

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Software defined networking for security enhancement in wireless mobile networks

Aaron Yi Ding [a,b], Jon Crowcroft [b,*], Sasu Tarkoma [a], Hannu Flinck [c]

[a] University of Helsinki, Finland
[b] Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge, United Kingdom
[c] Nokia Solutions and Networks, Finland

ARTICLE INFO

Keywords:
Software defined networking
Security
Wireless mobile networks

ABSTRACT

In recent years we have seen a fast change in the networking industry: leading by the Software Defined Networking (SDN) paradigm that separates the control plane from the data plane to enable programmability and centralized control of the network infrastructure, the SDN design not only simplifies the network management but also accelerates the innovation speed of deploying advanced network applications. Meanwhile, the landscape of the wireless and mobile industry is changing dramatically as well. Given the advance of wireless technologies such as 4G and WiFi offering a pervasive Internet access, the traffic growth from the smartphone-alike devices has placed an increasing strain on the mobile network infrastructure and infringed the profit. Since the demand is increasing together with the growth of mobile users, the incumbent legacy infrastructure is already calling for an upgrade to overcome its existing limitations in terms of network management and security. In this paper, we advocate that the way forward is to integrate SDN and fully utilize its feature to solve the problem. As the security issue has raise serious concern in the networking community recently, we focus on the security aspect and investigate how to enhance the security with SDN for the wireless mobile networks.

1. Introduction

The Software Defined Networking (SDN) is a disruptive and innovative force in the networking industry that affects almost every player including network operators, equipment vendors, Internet service providers and cloud service providers. With SDN, the low-level device configuration and management can be handled by the centralized software controller which facilitates the upgrade of functionality and debugging. By managing and distributing the network state with a system perspective, SDN frees the administrators from mining the complex protocol specifications with agility and flexibility to control the networks. The SDN-enabled Network Functions Virtualization (NFV) also makes it possible for the Internet and cloud service providers to deliver their differentiation advantage in the market through service improvement in terms of Quality of Service (QoS) and security.

Behind the SDN paradigm that separates the control and data plane, SDN delivers four visible features to the networking field:

- Central control and coordination – the logically centralized control model is a key part of the SDN architecture which mitigates the overhead from the traditional distributed mechanisms based on protocols. Although the centralized approach is often questioned for its scalability, it can deliver the state and policy changes more efficiently than the distributed methods in a managed

* Corresponding author.
E-mail address: jon.crowcroft@cl.cam.ac.uk (J. Crowcroft).

http://dx.doi.org/10.1016/j.comnet.2014.03.009
1389-1286/

domain. The coordination feature also makes it possible that when one of the controllers fails, other standby ones can take over the management tasks to avoid service breakage, which poses a great challenge for the distributed approach.

- Programmability – for both the control plane and the data plane, SDN makes implementation and deployment of the new functionality faster and easier, and hence speeding up the innovation at both hardware and software level. This agility can reduce the cost for service and network providers in terms of Operational Expenditure (OPEX) as the management can be powered by SDN applications in an automatic manner. By avoiding the unnecessary replacement of the underlying hardware through software update, it can also bring down the Capital Expenditure (CAPEX) and facilitate the adoption by the cloud providers.
- Virtualized abstraction – the layered design of SDN hides the complexity of hardware devices from the control plane and SDN applications. Through virtualized abstraction, SDN allows the managed network to be divided into virtual networks that share the same infrastructure but are governed by different policy and security requirements. Such flexibility greatly promotes the sharing, aggregation and management of available resources and enables dynamical reconfiguration and changes of policy.
- Openness – the open standards of SDN such as OpenFlow help build and develop open sourced communities that attract brain power and speed up the innovation. Such openness combined with programming APIs can promote the networking research by allowing researchers to experiment with novel ideas through fast prototyping and testing. It also benefits the interoperability with the legacy infrastructure and allows different operators and providers to collaborate through the SDN framework.

Since SDN allows a granular control of network and services through its abstraction of the underlying hardware, it meets the urgent need from the mobile networks that are going through a fast change to simultaneously operate over multiple wireless technologies (e.g., 4G and WiFi) in order to accommodate the radical growth of data traffic. There are several studies and proposals [1–7] exploring the potential of SDN in wireless mobile networks. As illustrated in Fig. 1 of an envisioned SDN-enabled wireless mobile networks, the current trend of convergence in such networks can benefit from SDN to enhance resource utilization, network management and security in the multi-service and multi-vendor environment.

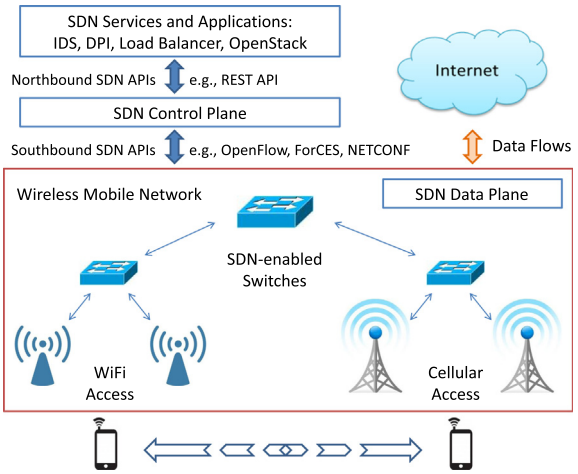


Fig. 1. SDN-enabled wireless mobile networks.

As discussed in [8,15], the security of SDN deserves our special attention for the challenges it brings and also the opportunities to enhance the network security. In this article, we review the recent work on SDN for wireless mobile networks and discuss how SDN solutions can improve security in such a dynamic environment. By surveying the SDN-based security solutions, we identify the design goals and describe our approach of utilizing SDN for security enhancement in wireless mobile networks.

2. SDN for wireless mobile networks

As wireless mobile networks are becoming the major channel to access Internet services, there is an urgent need to keep up with the pace of user growth and the scale of services. For instance, the recent demand of network capacity for mobile data traffic is far exceeding the supply of incumbent networks. At the same time, services also evolve in both variety and complexity. Since operators are limited by the commercial budget and the operation cost, it is extremely hard, if not impossible, to keep up with such speed while still cost-effectively upgrading the infrastructure, delivering service updates, and improving the end user experience under the existing infrastructure.

As highlighted in Table 1, we describe in this section the latest SDN solutions for wireless mobile networks that aim to address the challenges. The range of discussion covers the cellular and the WLAN environment, from the angle of core infrastructure and edge access.

Table 1
SDN solutions for wireless mobile networks.

	WWAN cellular environment	WLAN campus/enterprise environment
Core infrastructure	CellSDN [1]: Cellular SDN architecture design SoftCell [2]: Scalable core network design	OpenRoads [5]: Open wireless infrastructure on campus Odin [6]: Programmable platform for enterprise WLANs
Edge access	SoftRAN [3]: SDN control plane for radio access OpenRadio [4]: Programmable wireless data plane	OpenAPI [7]: Open SDN APIs for access network virtualization OpenRadio [4]: Programmable wireless data plane

2.1. Cellular networks

The existing cellular infrastructure has been criticized as being expensive and inflexible, suffering from complex control plane protocols and vendor-specific configuration interfaces [1,2]. In order to simplify the management of cellular data networks, the pioneering project CellSDN [1] proposes a SDN design for the cellular core infrastructure. Because applying SDN to cellular environment needs to address several challenges, including user mobility and real-time adaptation, a set of necessary extensions are identified for the key elements of CellSDN architecture. On the proposed controller extension, policies of subscriber attributes are translated into switch rules that match on packet headers. A local control agent is introduced on the switch to alleviate the scalability issue of central controlling by performing localized actions guided by the control platform.

By pushing forward the high-level design of CellSDN, SoftCell [2] presents a detailed scalable architecture design to support fine-grained policies in cellular core networks. With the controller handling low-level details such as switch location and network identifier, SoftCell adopts a set of service policies as a high level of abstraction based on subscriber attributes and applications. The service policies include priority, service action, and predicates. To handle network dynamics and enable fine-grained policies at scale, SoftCell achieves scalability by extending both the control and data plane. In the control plane, SoftCell uses local software agents to cache packet classifiers and policy tags in order to reduce the load of the main controller. In the data plane, SoftCell pushes packet classification to the access switches and apply multi-dimensional forwarding rule aggregation to minimize the state in the core network.

For the cellular edge access, SoftRAN [3] and OpenRadio [4] are the latest proposals aiming at bringing the power of SDN to innovate the wireless access domain. SoftRAN focuses on the control plane design by abstracting multiple base stations into a virtual big base station. A 3D resource grid is defined by SoftRAN to allow operators to manage the radio resources within a geographical area through three dimensions – time, frequency, and base station index. The SoftRAN controller maintains a RAN information base (RIB) which can be accessed by various control modules for radio resource management. The RIB consists of essential information to be updated by the controller, such as the interference map, flow record, and network operator preference. As the radio element has a more timely view of the local state than the remote controller, SoftRAN further optimizes the control decision by splitting the control functionality between the central controller and the radio elements.

OpenRadio [4] proposes a data plane solution to enable programmability through modular and declarative programming interfaces across the wireless stack. As the existing wireless infrastructure suffers from the closely coupled hardware, OpenRadio aims at decoupling the protocol definition from the hardware and providing a software abstraction layer to enable the programming of the MAC and physical layer. The main idea is to decompose of wireless protocols into processing plane and decision plane where the processing plane includes actions and the decision plane includes rules. Owing to its design generality, OpenRadio can be applied to both the cellular and the WiFi environment.

2.2. WLAN environment

OpenRoads [5] is the first SDN solution that is deployed on campus using OpenFlow and virtulization to decouple mobility from physical network and allow multiple providers to control and configure underlying infrastructure concurrently. The OpenRoads platform aims at enabling experimental research by using open-source controller and extend it to control and capture wireless events such as host-AP association. The greatest feature of OpenRoads is its openness that all the tools used and developed in the project are freely available under open-source licenses to encourage the contributions from the community.

For the enterprise infrastructure, Odin [6] develops a SDN platform targeting at the enterprise wireless local area networks. By building a light virtual access point (LVAP) abstraction, Odin can virtualize the association state and separate them from the physical access point to simplify the client management. The design of LVAP enables the operators and developers to program and deploy typical WLAN services as network applications running on top of Odin. As an example application, Odin supports efficient handoff by using LVAP to avoid additional message exchange at the client. The Odin mobility manager can monitor the receiver signal strength through local agents to guide the selection of handoff target AP. The key components of Odin are built on top of open-source OpenFlow controller Floodlight. The Odin development has been active and they aim to enrich the platform by creating more programming primitives such as LVAP.

For the edge access, OpenAPI [7] develops a system architecture to allow efficient control and sharing of WLAN resources by virtualizing the last-mile access infrastructure. The architecture specifies the interfaces between ISP, content provider, and end user to enable an open and agile service quality management. The proposed open APIs encourage all the parties to participate and collaborate, in which ISP can improve the monetization of their infrastructure resources on a flow basis without revealing network internals; the content provider can enhance business models by selectively tuning the service quality for different types of flows; and the end users can adjust the virtualization degree to meet the dedicated needs. A virtualization algorithm is developed by using the time elasticity of bulk transfer applications and the spatial overlap of WiFi coverage to achieve efficient resource usage.

For comprehensiveness, OpenRadio [4] also supports the WLAN environment for its open and flexible design.

3. SDN security

In this section we discuss the latest research on SDN security and categorize the selected proposals in terms of their target environment into four groups: enterprise networks, cloud & data center, home & edge access, and general design. We highlight in Table 2 the main contributions

of each proposal against a feature set we identify in the SDN context, including the modification of SDN plane, usage of OpenFlow, local optimization, consideration for the wireless mobile environment, and interoperability for cross-domain security and policy exchange.

As we focus on how to utilize SDN to enhance network security, it is worth noticing that the security concern for the SDN itself is also an important topic where the existing study [8] has identified seven threat vectors that may enable the exploit of SDN vulnerabilities and further propose a design to achieve secure and dependable SDN platform.

3.1. Enterprise networks

As one of the initial work of SDN, Ethane [9] redefines the network architecture for enterprise environment. By decoupling the control functionality away from traditional switches, the Ethane controller enforces the security by treating it as part of the central network management process and further regulates the authentication, bindings and access permission. As illustrated in Table 2, the Ethane design covers both control plane and data plane although the impact on data plane is mainly to simplify the switch functionality. Being the predecessor of OpenFlow, Ethane does not follow the existing OpenFlow standard at the time of proposing. It does not take into account the local optimization, the concern for wireless mobile environment, or the cross-domain interoperability.

Resonance [10] is another initiative to apply SDN to achieve dynamic access control in the enterprise/ campus environment. In order to overcome the difficulty of security enforcement based on traditional tools such as middleboxes and external monitoring systems, Resonance adopts a dynamic policy specification framework and uses OpenFlow-based programmable switches and controller to enable distributed network monitoring. The strength of Resonance comes from the dynamic access control in which network devices can treat traffic differently by following the controller's view toward end host's security class and state. The Resonance design involves control and data plane, and also utilizes the OpenFlow standard. However, it does not consider local optimization to improve scalability, nor does it meet the responsiveness and interoperability requirements of wireless mobile networks.

3.2. Home and edge access

The work of [11] presents the SDN-based implementation of four algorithms for Anomaly Detection System (ADS) and advocates that such programmable solution deployed in a home network environment can achieve more accurate identification of malicious activity comparing to the one that is deployed at the ISP. Their SDN-based solution can also alleviate the load of ISP from monitoring a large number of home networks and promote collective detection of global network problems by feeding the monitoring results to external entities. This work requires modification of the SDN control plane. It does not consider features of local optimization, mobile scenario, or cross-domain interoperability.

Targeting at protecting end hosts on the edge access, the OpenFlow Random Host Mutation (OF-RHM) [12] uses OpenFlow to develop a proactive moving target defense technique to hide the end hosts from adversaries such as scanners. The protection can counter the scanning attack through the random and unpredictable mutation of host IP addresses based on its probability algorithm. The OpenFlow-based proposal utilizes the SDN central controller to assign a virtual IP to the host which can be mapped to the real host IP. Since the real IP remains the same, OF-RHM operation is transparent to the end hosts. As shown in Table 2, OF-RHM uses the OpenFlow controller and does not consider features of local optimization, mobile scenario, or cross-domain interoperability.

3.3. Cloud and data center

NetFuse [13] is a new proposal for cloud and data center environment to protect it against traffic surges that origin from either security attacks, operator errors, or routing misconfiguration. NetFuse uses both passive listening and adaptive active query to enable effective monitoring of network status. It utilizes a multi-dimensional aggregation to find the suspicious flow clusters. To improve efficiency and responsiveness, NetFuse further adopts a toxin-antitoxin mechanism to adaptively shape the flow rate according to application feedback. The design is realized as a proxy between the OpenFlow switches and the controller. As shown in Table 2, NetFuse follows the OpenFlow standard but does not modify the control and data plane. It delivers local optimization by relieving the heavy load from the controller such as flow redirection, delay injection, and blocking. NetFuse does not consider the features of mobile and cross-domain.

CloudWatcher [14] utilizes the advantage of SDN to build a framework that can efficiently monitor services in large and dynamic cloud networks. The proposed scripting language enables operators to employ security monitoring as a service in a convenient fashion. CloudWatcher includes four routing algorithms to optimally reroute traffic to a security monitoring node. The framework consists of three key components: device and policy manager, routing rule generator, and flow rule enforcer. CloudWatcher does not demand changes on control or data plane, and utilizes the routing algorithms to optimize security monitoring. However, it does not consider the features of mobile and cross-domain.

3.4. General design

AVANT-GUARD [15] is a new framework to address two security challenges for SDN-enabled networks. The first goal is to secure the interface between the control plane and the data plane and shield it from knowledgeable adversaries. To achieve this, AVANT-GUARD proposes a connection migration technique on the data plane to protect the control plane from the saturation attacks. The second goal is to improve responsiveness so that security applications can efficiently access network statistics to response to threats. AVANT-GUARD address this by creating actuating triggers that can be inserted by the control plane

to register asynchronous call back and as well as add conditional flow rules that are activated when a predefined trigger condition is detected. As shown in Table 2, AVANT-GUARD involves both data and control plane and is based on the OpenFlow standard. It also provides optimization by extending functionality at the data plane. No description is given for wireless mobile environment nor for the interoperability.

FRESCO [16] builds a development framework to facilitate the design and composition of various SDN-enabled security applications. It consists of a FRESCO application layer and a security enforcement kernel. The application layer in FRESCO provides a development environment and a resource controller through which developers can use FRESCO scripting language to compose security functions. The FRESCO security enforcement kernel is integrated to the OpenFlow controller to ensure the conformance of rules and avoid conflicts. Targeting the general environment, FRESCO does not require changes on the data plane, and does not consider the features of mobile environment and cross-domain interoperability.

OpenWatch [17] targets at adaptive flow counting by using SDN's feature to break the binding between forwarding and counting. It proposes a dynamic rule update algorithm and a prediction based scheme to zoom into flow space via temporal and spatial dimensions. OpenWatch can also reduces the number of rules on the data plane through its greedy rule assignment algorithm. As shown in Table 2, it is based on OpenFlow standard and relies on control plane modification. However, OpenWatch does not consider other features.

NIDS Arch. [18] proposes a general network intrusion detection system (NIDS) to promote the scaling of NIDS hardware and augment existing NIDS deployment. A lightweight shim layer is designed to leverage three scaling opportunities including on-path distribution to split the responsibilities, replicating traffic to NIDS clusters, and aggregating intermediate results to split expensive NIDS processing. By using a logically centralized management module to configure NIDS elements, this design follows the SDN principle although not relying on OpenFlow standards. The design space touches both control and data plane. Optimization is considered in the proposal by replication and aggregation. However, it does not cover the mobile scenario nor the cross-domain interoperability.

FleXam [19] proposes a flexible sampling extension for OpenFlow to promote the development of security applications such as monitoring. To overcome the limitation of existing OpenFlow mechanisms to access packet-level information such as port manipulation and mirroring, FleXam enables flexible sampling by enabling controller to specify which packets shall be sampled and what part of packet shall be selected, and to where it shall be sent. Packets can be sampled either stochastically or deterministically and thus making it flexible to meet the needs of different applications. The design is fully implemented on data plane and take into account the ptimization and the dynamics of the mobile environment, although not applicable to cross-domain interoperability.

4. Enhanced security in wireless mobile networks with SDN

Network convergence is the trend for wireless mobile networks where operators will integrate diverse wireless technologies (e.g., 4G and WiFi) to the network infrastructure. This creates a challenge toward interoperability as how to manage the multi-vendor physical devices that use different configurations under various policy and security requirement in a multi-operator environment. As end users often move across different networks managed by different operators, such mobility brings complexity to the network management in terms of interpreting inter-domain policy to guarantee consistent security in a dynamic and efficient manner.

SDN provides the virtualized abstraction that gives a convenient way to hide the complexity of various wireless protocols and topology. The programmability and flow model of SDN also facilitate granular policy control, flexible traffic aggregation and partition. These functional features and its openness make SDN suitable for the upcoming wireless mobile environment.

According to our investigation on SDN for security and its presence in the wireless mobile networks, as highlighted in Tables 1,2, we observe there is a lack of concern for SDN security in wireless and mobile domain. The OpenFlow API and its north bound interfaces already provide a good foundation for innovative solutions on top of the existing SDN framework, especially for security elements. We share our perspective and present our design to enhance security in this dynamic and fast changing area.

4.1. Challenge and requirement

The feature set in Table 2 provides several desired items. Based on them, we identify the design challenges and outline the requirements.

- Mobility and Roaming: The mobility of users results in roaming between networks and potentially across different access technologies such as 4G and WiFi. This dynamic change adds complexity to the diagnose and detection of anomaly activities and as well as the security credential exchange.
- Monitoring Overhead: The OpenFlow-based monitoring schemes suffer from limitation in terms of high overhead and incomplete sample information. FleXam [19] provides a good example toward this challenge.
- Multi-Access and Multi-operator: The operational environment consists of different technolgoies and operators leading to complex negotiation process, privacy concern, and potential conflicting policy and QoS requirement that pose a challenge to the security enforcement.
- Deployment: Although SDN has openness in its nature, any solution deployed needs to face the challenge of backward compatibility and interoperability as operators need to maintain different generations of technologies (e.g., 3G and 4G) and intercommunicate with other providers.

For a sound SDN design for security enhancement, we need to meet several requirement:

Table 2
SDN-enabled security solutions.

Proposal	Target environ.	Main contributions	Design features				
			SDN plane	OF-based	Local optim.	Mobile	Cross-domain
Ethane [9]	Enterprise	First SDN design, deployment experience	Control & data	No	No	No	No
Resonance [10]	Enterprise	Access control, policy specification framework	Control & data	Yes	No	No	No
ADS Revisit [11]	Home network	Algorithm evaluation, implementation experience	Control	Yes	No	No	No
OF-RHM [12]	Edge access	Random host mutation, protocol design	Control	Yes	No	No	No
NetFuse [13]	Cloud/ DC	Monitoring, aggregation adaptive rate limiting	None	Yes	Yes	No	No
CloudWatcher [14]	Cloud/ DC	Monitoring, routing algorithms, policy script	None	Yes	Yes	No	No
AVANT-GUARD [15]	General	Actuating trigger, connection migration	Control & data	Yes	Yes	No	No
FRESCO [16]	General	Developing platform for security applications	Control	Yes	No	No	No
OpenWatch [17]	General	Flow counting algorithm, adaptive design	Control	Yes	No	No	No
NIDS Arch. [18]	General	Scalable NIDS design, traffic replication, aggregation	Control & data	No	Yes	No	No
FleXam [19]	General	Flexible sampling technique, low overhead	Data	Yes	Yes	Yes	No

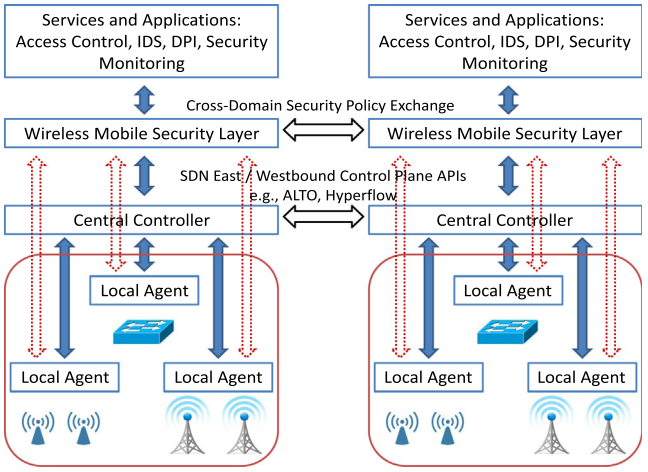


Fig. 2. Security enhancement framework for wireless mobile networks.

- Interoperability: Handling information exchange between different elements are crucial for SDN security design for wireless mobile environment. The recent trend of cellular offloading also makes this relevant since WiFi and Cellular management are used to be separate, especially the security part. Traditional distributed protocol is incapable for this due to the complexity and privacy issues.
- Responsiveness: Processing events in wireless mobile networks should be timely, either in reactive or proactive manner. Efficient triggering and local optimization are valuable.
- Compatibility: To maximize the value of openness, using a standard API is required, such as OpenFlow.
- Adaptation: Due to mobility and network condition changes, a design should be adaptive by monitoring and efficiently detecting events both in the network and from user activities.
- Simplicity: To promote deployability and encourage contributions from the community, a proposal should avoid complex extension on hardware-based data plane and OpenFlow protocol extension.

4.2. System design and use cases

To illustrate how to enhance security in wireless mobile networks, we propose a SDN-based framework as depicted in Fig. 2. The key elements in our framework include local

agents, central controller, and security layer for wireless mobile networks.

The local agents are deployed close to the wireless edge access to meet the requirements of responsiveness, adaptation, simplicity. Inspired by [6,19], Optimization techniques are employed by local agents including flow sampling, tracking client records and mobility profile. Instead of inserting actuation triggers in the data plane, local agents take the responsibility to adaptively query information from the underlying devices and report to the controller. This provides transparency to both data plane and controller and hence alleviating the monitoring load on the central controller.

The central controller is the management entity running OpenFlow to control switches and OpenFlow-enabled wireless devices. To improve compatibility and simplicity, our design adopts only the mature and open standards to manage the network.

The security layer resides on top of the control plane and aims to meet the requirements of interoperability, compatibility, and simplicity. For instance, it adopts the design of [20] to improve interoperability by allowing different operational networks to exchange security policy in the form of policy predicates through the channel between the security layers, as showin in Fig. 2.

We use three types of communication channels in our framework. As illustrated in Fig. 2, the blue lines represent the OpenFlow based channels between standard data plane and control plane. The red lines are customized channels for security purposes such as reporting mobile client's activity and tuning wireless devices configuration. The white lines are logical channels for cross-domain communication through which security credentials can be exchange and interpreted while respecting the internal privacy.

In brief, our framework aims at the wireless mobile environment. We enhance the scalability by using local agents to process the local events. Since reaction must be fast in the wireless mobile environment, the local progressing reduces the latency from data plane to controller and therefore delivers better performance. We further utilize the security layer to achieve interoperability across different access domains that are managed by different operators. We use the naming of predicate routing design to achieve the security policy exchange between those [20].

We highlight three potential use cases for our design.

- Complementing an Intrusion Detection System (IDS) – The local agents will regulating monitoring tasks by using triggers and flexible sampling to fetch necessary information from edge network and end host and feeding such information to IDS service such as Snort.
- Prevention of DoS near the wireless edge – avoiding resource waste such as spectrum, if the malicious traffic are only dropped in the core network switches rather than dropped as early as possible. The local agent coordinates the operation by installing rules to drop packets and inform the central controller.
- Secure handoff for mobility – Proactively deliver security keys and credentials to target networks to improve efficiency for handoff.

5. Concluding remarks

The maturity of OpenFlow standards and fast development of SDN have made the concept of SDN widely accepted by the mobile industry. For the advantages of SDN such as programmability, abstraction, and openness, we advocate that SDN can enhance security in wireless mobile networks through novel design. Based on our investigation of existing solutions, we highlight the key elements and sketch out our design. As part of our on-going work for the security enhancement framework, we believe this study can shed light on how we use SDN to improve network security and promote the adoption of SDN to the future wireless mobile networks.

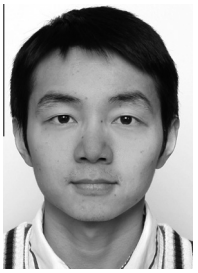
Acknowledgement

The Ph.D. research of Aaron Yi Ding is supported by the Academy of Finland and Nokia Foundation.

References

[1] L.E. Li, Z.M. Mao, J. Rexford, Toward software-defined cellular networks, in: Proceedings of IEEE EWSDN, 2012.
[2] X. Jin, L.E. Li, L. Vanbever, J. Rexford, SoftCell: scalable and flexible cellular core network architecture, in: Proceedings of ACM CoNEXT, 2013.
[3] A. Gudipati, D. Perry, L.E. Li, S. Katti, SoftRAN: software defined radio access network, in: Proceedings of ACM HotSDN, 2013.
[4] M. Bansal, J. Mehlman, S. Katti, P. Levis, OpenRadio: a programmable wireless dataplane, in: Proceedings of ACM HotSDN, 2012.
[5] K. Yap, et al., Blueprint for introducing innovation into wireless mobile networks, in: Proceedings of ACM VISA, 2010.
[6] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, T. Vazao, Towards programmable enterprise WLANs with odin, in: Proceedings of ACM HotSDN, 2012.
[7] V. Sivaraman, T. Moors, H.H. Gharakheili, D. Ong, J. Matthews, C. Russell, Virtualizing the access network via open APIs, in: Proceedings of ACM CoNEXT, 2013.
[8] D. Kreutz, F. Ramos, P. Verissimo, Towards secure and dependable software-defined networks, in: Proceedings of ACM HotSDN, 2013.
[9] M. Casado, M.J. Freedman, J. Pettit, J. Luo, N. McKeown, S. Shenker, Ethane: taking control of the enterprise, in: Proceedings of ACM SIGCOMM, 2007.
[10] A.K. Nayak, A. Reimers, N. Feamster, R. Clark, Resonance: dynamic access control for enterprise networks, in: Proceedings of ACM WREN, 2009.
[11] S.A. Mehdi, J. Khalid, S.A. Khayam, Revisiting traffic anomaly detection using software defined networking, in: Proceedings of RAID, 2011.
[12] J.H. Jafarian, E. Al-Shaer, Q. Duan, OpenFlow random host mutation: transparent moving target defense using software defined networking, in: Proceedings of ACM HotSDN, 2012.
[13] Y. Wang, Y. Zhang, V. Singh, C. Lumezanu, G. Jiang, NetFuse: short-circuiting traffic surges in the cloud, in: Proceedings of IEEE ICC, 2013.
[14] S. Shin, G. Gu, CloudWatcher: network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?), in: Proceedings of IEEE ICNP NPSec Workshop, 2013.
[15] S. Shin, V. Yegneswaran, P. Porras, G. Gu, AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks, in: Proceedings of ACM CCS, 2013.
[16] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, M. Tyson, FRESCO: modular composable security services for software-defined networks, in: Proceedings of NDSS, 2013.

[17] Y. Zhang, An adaptive flow counting method for anomaly detection in SDN, in: Proceedings of ACM CoNEXT, 2013.
[18] V. Heorhiadi, M.K. Reiter, V. Sekar, New opportunities for load balancing in network-wide intrusion detection systems, in: Proceedings of ACM CoNEXT, 2012.
[19] S. Shirali-Shahreza, Y. Ganjali, Efficient implementation of security applications in OpenFlow controller with FleXam, in: Proceedings of IEEE Symposium on High-Performance Interconnects, 2013.
[20] T. Roscoe, S. Hand, R. Isaacs, R. Mortier, Jardetzky Paul, Predicate routing: enabling controlled networking, ACM SIGCOMM Comput. Commun. Rev. (CCR) 33 (1) (2003) 65–70.



Aaron Yi Ding is a Ph.D. candidate supervised by Prof. Sasu Tarkoma and Markku Kojo at the University of Helsinki, with Prof. Jon Crowcroft being his external advisor at Cambridge. He obtained his MSc with distinction in computer science from the University of Helsinki in 2009. Since 2007 he has been employed for the R&D projects collaborating with Nokia, NSN, and TeliaSonera with 7+ years experience. He is a recipient of the Cambridge Visiting Scholarship and Nokia Foundation Scholarship.

Jon Crowcroft has been the Marconi Professor of Communications Systems in the Computer Laboratory since October 2001. He has worked in the area of Internet support for multimedia communications for over 30 years. Three main topics of interest have been scalable multicast routing, practical approaches to traffic management, and the design of deployable end-to-end protocols. Current active research areas are Opportunistic Communications, Social Networks, and techniques and algorithms to scale infrastructure-free mobile systems. He leans towards a "build and learn" paradigm for research.
He graduated in Physics from Trinity College, University of Cambridge in 1979, gained an M.Sc. in Computing in 1981 and Ph.D. in 1993, both from UCL. He is a Fellow the Royal Society, a Fellow of the ACM, a Fellow of the British Computer Society, a Fellow of the IET and the Royal Academy of Engineering and a Fellow of the IEEE.
He likes teaching, and has published a few books based on learning materials.

Sasu Tarkoma received his M.Sc. and Ph.D. degrees in Computer Science from the University of Helsinki, Department of Computer Science. He is full Professor at University of Helsinki, Department of Computer Science and Deputy Head of the Department. He has managed and participated in national and international research projects at the University of Helsinki, Aalto University, and Helsinki Institute for Information Technology (HIIT). His interests include mobile computing, Internet technologies, and middleware. He is Senior Member of IEEE.

Hannu Flinck is a Research Manager at Nokia Solutions and Networks, Espoo, Finland. He received his M.Sc. degree (1986) and Lic.Tech. degree (1993) in Computer Science and Communication Systems from Helsinki University of Technology, Finland. His current research agenda includes cloud technology, SDN and content delivery in mobile networks.