IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 12, 2017, accepted October 29, 2017, date of publication November 24, 2017, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2773647

Secure Monitoring of Patients With Wandering Behavior in Hospital Environments

VIJAY VARADHARAJAN[1], (Senior Member, IEEE), UDAY TUPAKULA[2], (Member, IEEE), AND KALLOL KARMAKAR[2], (Student Member, IEEE)

[1]Faculty of Engineering, The University of Newcastle, Callaghan, NSW 2308, Australia
[2]School of Electrical Engineering and Computing, The University of Newcastle, Callaghan, NSW 2308, Australia

Corresponding author: Uday Tupakula (uday.tupakula@newcastle.edu.au)

ABSTRACT Today there is considerable interest for making use of the latest technological advancements for several healthcare applications. However, there are several challenges for making use of different technologies for healthcare applications. In particular, there is a need to ensure that the healthcare related services receive priority during events, such as legitimate failures of devices, congestion, and attacks in the networks. In this paper, we discuss some of the requirements for making use of technology for healthcare applications and propose techniques for secure monitoring of patients with wandering behavior in a hospital or elderly care environment. One of the aims of our work is to use technology for secure monitoring of patients with wandering behavior to keep them away from danger, or detect if the behavior of the patient violates the policies of the hospital, or even violates privacy policies of other patients. Our approach makes use of software defined networking (SDN), Wireless LAN (WLAN), and wearable devices for the patients. Our approach incurs low cost since WLAN is widely deployed. However, there are some challenges for making use of WLAN for monitoring dementia patients, since it is primarily used for accessing the Internet and its open nature is vulnerable to different types of security attacks. Hence we make use of SDN to solve some of these challenges and provide priority for the monitoring services. We have developed a security application for an SDN controller that can be used to enforce fine granular policies for communication between the hosts, real time location tracking of the patients, and deal with attacks on the hospital networks. The policy-based security enforcement helps to differentiate healthcare related traffic from other traffic and provide priority to the healthcare traffic. The real time location tracking detects wandering by patients and if necessary can raise alarms to the staff. The attack detection component makes use of attack signatures and behavior-based intrusion detection to deal with attacks on hospital networks. We will also present the prototype implementation of our model using ONOS SDN controller and OpenFlow Access Points.

INDEX TERMS Secure healthcare, dementia, wandering behaviour, patient tracking, software defined networking, SDN, security attacks, WLAN localisation, intrusion detection.

I. INTRODUCTION

Wandering behaviour is frequently seen in older people with cognitive impairment. For instance, Dementia [1]–[4] is a brain disease which affects the normal brain functioning of the patient. In severe cases, the patient finds it extremely difficult or completely loses control to perform day to day duties. In Dementia the size of the brain decreases rapidly with time, which causes these inabilities with natural human behaviour. Most common types of dementia are, Alzheimer's, vascular dementia, Parkinson's disease dementia and mixed dementia. Gene and age are the most common factors that cause Dementia. Medical science does not hold any cure for this diseases till to date. Depending on the severity of this disease life span of a patient can vary from 5-20 years. Alzheimer's is one of the most common forms of dementia which is followed by vascular dementia which occurs after a stroke. Vascular dementia [5] results due to blockage of major blood vessels in the brain and can severely impact the mental ability of the patient. Patients can have varying symptoms depending on the damage of the blood vessels. For instance, such patients can have one or more of the following symptoms: confusion, vision loss, wandering, trouble with speaking and understanding.Since the dementia patients can have progressive change of behaviour, it is challenging task

for the hospitals to deal with such patients with specific requirements.

In some cases, the patients with no serious changes in behaviour can feel violation of their privacy if a nurse is used for continuous physical monitoring of the patients. In some cases, the patients with serious change of behaviour need continuous monitoring. For example, the patients with serious change in the behaviour can leave the hospital premises and get lost [6]. Also such lost patients will not be able to convey any information due to the conditions caused by the disease. In some cases, the patients can get into locations within the hospital that is harmful to them such as laboratories with hazard material. In some cases, the patients can violate the hospital rules and privacy of other patients by entering into other rooms. Failure to detect such events can lead to havoc or security breach in such environments. However it is not feasible for the hospitals for continuous physical monitoring of the patients with wandering behaviour due to financial constraints and severe shortage of nursing staff. Also it is not efficient to make use of the nursing staff to monitor a single patient. Hence there is need to design new techniques to suite these specific requirements. In this paper, unless specifically stated, patient refers to patient with wandering behaviour.

Currently there is considerable interest for making use of different heterogeneous technologies for healthcare applications [7]–[9]. However, there are several challenges for making use of different technologies for healthcare applications. First there is a need to consider the specific requirements for the healthcare application. Then there is a need to consider the challenges with specific technologies used for the healthcare application. In particular, there is a need to ensure that the healthcare related services receive priority during events such as legitimate failures, congestion and attacks.

In this paper, we propose techniques for secure monitoring of dementia patients in hospital or elderly care environment. We propose SDN-based techniques for secure monitoring of patients in hospital environment. Our model enables the security administrators to makes use of the global network knowledge available at the SDN controller to enforce fine granular policies for communication between the hosts, real time location tracking of the patients and deal with the attacks in the hospital networks. Our model helps to track the location of the patients with wandering behaviour and raise alarms to the concerned staff if the location of the patients is violating any of the security and privacy policies. Furthermore, our model enables to differentiate healthcare related traffic from other traffic and provide priority to the healthcare traffic during the events such as congestion and attacks in the hospital network.

The paper is organised as follows. Section 2 gives a brief overview of the SDN technology. In Section 3, we present our approach and operation of our model. Section 4 presents the implementation details and some specific scenarios to demonstrate the operation of our model. Section 5 presents some of the related work and Section 6 concludes.

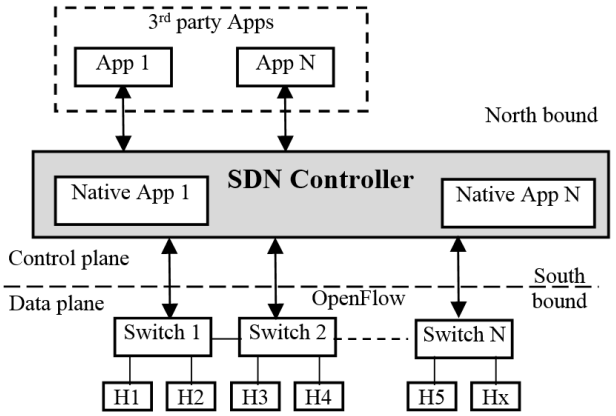

FIGURE 1. SDN overview.

II. SDN OVERVIEW

Software Defined Networking (SDN) [10] is a promising technological advancement in the networking world. SDN simplifies the tasks of the network administrators for managing complex networks. Traditional networking devices have the control plane and data plane integrated into the same device. Also different network product vendors used proprietary protocols for configuring and managing these devices. Hence administrators had to manually configure these traditional networking devices which is often a slow process and one of main cause for the occurrence of errors. The innovation in SDN is the separation of the control plane from the data plane and it enables programmable networks. There are significant benefits with this separation of control plane from the data plane. The control functionality for the whole network can be implemented on a logically centralised device using standard computers and also switches become simple forwarding devices where the flow rules can be directly programmed from the Controller. This will help to handle the complexity in the current networks, minimise errors and enable innovation in networks.

A sample architecture representing different components in control plane and data plane is shown in Figure 1. The Controller is a logically centralised (which can be distributed in practice) device with native applications for managing the networks. Several controllers [11] such as NOX, POX, Beacon, Floodlight and ONOS are currently available. Applications are hosted on the North Bound Interface of the Controller. Hence any new applications can be developed and hosted on this interface. Switches are hosted in the dataplane. The interface between the controller and switches is called as south bound. Protocols such as OpenFlow [10], sflow, snmp can be used for communication between the devices in the control plane and the data plane. An OpenFlow compatible switch consists of secure communication channel which permits dynamic configuration of the flow rules by an SDN Controller.

In traditional networks, the switches make a routing decision depending on the local configuration of the device to

route the flows from source to the destination. In SDN, switches simply forward the new flow requests to the controller. The Controller makes the routing decision based on the global knowledge of the networks and configures the corresponding switches to enable communication between the source host and the destination host. Hence in this paper we make use of global network knowledge and per flow decision making of the SDN Controller to deal with the attacks and provide priority for the real time location tracking of the dementia patients.

III. OUR APPROACH

In this section we will first consider some of the requirements for our model. Then we will present the operation of our model and provide a discussion related to our model.

A. REQUIREMENTS

- Although there is a need for continuous location monitoring of the patients with wandering behaviour, note that there can be several other patients in hospitals that may not need such location tracking. So usage of sophisticated technologies for real time location monitoring of the patients can incur considerable cost for the deployment of the technology and also for training of the staff for the usage of the technology.
- Tracking the location of the patients is possible on the wearable devices and from the network. Our design choice is to use network based tracking due to limited battery resources of the wearable devices and also due to the inability of the dementia patients. For example, providing location information on the wearable device may not be of much help for the dementia patients with loss of memory and/or visibility. Device based tracking will also result in the increase of the cost of the wearable device since it requires additional display mechanisms on the wearable device. Hence network based tracking is more desirable.
- There can be progressive change of behaviour of the patients. For instance, the early signs of dementia can be very subtle and then there can be variation of behaviour over a period of time such as frequent memory loss, confusion, personality change and loss of ability to perform daily tasks. Hence the proposed techniques should not depend on the behaviour of the patients.
- Events such as congestion and attacks can significantly degrade the availability of services in the hospital networks. Hence there is need for techniques to deal with such events to ensure availability of the services and provide high priority to the traffic related to patient location monitoring.

B. OVERVIEW

As shown in the Figure 2, we consider a scenario where SDN is used for managing the hospital network (wired and wireless). Services related to the hospital operations such as billing and other administrative services are provided in the wired network. The WLAN is used for real time monitoring of the dementia patients and also for providing Internet services to other users such as patients without dementia, guests and hospital staff. OF-APs are placed at different locations within the layout with overlapping range and there are some attack detection components (not shown) to monitor the traffic for different activities such as congestion of the medium, detection of rogue access points broadcasting unauthorized SSID, and traffic matching with attack signatures.

We assume that the SDN Controller is a trusted entity within the domain and there are mechanisms for ensuring security and high availability of the Controller. For example, techniques such as [12]–[14] can be used for making controller robust against the attacks and to ensure high availability of the Controller. We assume that patient's information which is provided during admission is mapped to the wearable device ID and the devices are tagged to the patient. A shared secret is used for authentication of the wearable device to the hospital network. There is a need to ensure that the devices cannot be easily detached by the patients. Hence tracking the location of wearable device corresponds to the actual location of the patient. Each patient will be allocated a minimum of two wearable devices to ensure continuous tracking of the patients. For example, the wearable devices may have to be detached from the patients for recharging the battery. Hence there is a need for an additional device for continuous tracking of the patients.

We have developed a Security Application for an SDN Controller that can be used to enforce fine granular policies for communication between the hosts, real time location tracking of the patients and deal with the attacks in the hospital networks. The Security Application can be implemented on any of the SDN Controllers with minor modifications. The policy based security enforcement helps to differentiate healthcare related traffic from other traffic and provide priority to the healthcare traffic. The real time location tracking helps to detect if the location of the patients is violating any of the hospital policies and raise alarms to the concerned staff. The attack detection component makes use of attack signatures and behaviour based intrusion detection to deal with the attacks in hospital network. In the following subsections, we provide detailed discussion on the security application, location tracking of the patients and attack detection in hospital networks.

C. SECURITY APPLICATION

SDN controller has a domain wide knowledge of all the devices in the network and network topology with interconnections between the devices. Our Security Application runs over the SDN controller. The Security Application makes use of the information available in the SDN controller and also stores some additional information such as policies for securing the communication of the devices and policies for detecting the attacks in SDN domain.

Figure 2 shows the different components of the Security Application. They are: 1) Access Manager, 2) Policy

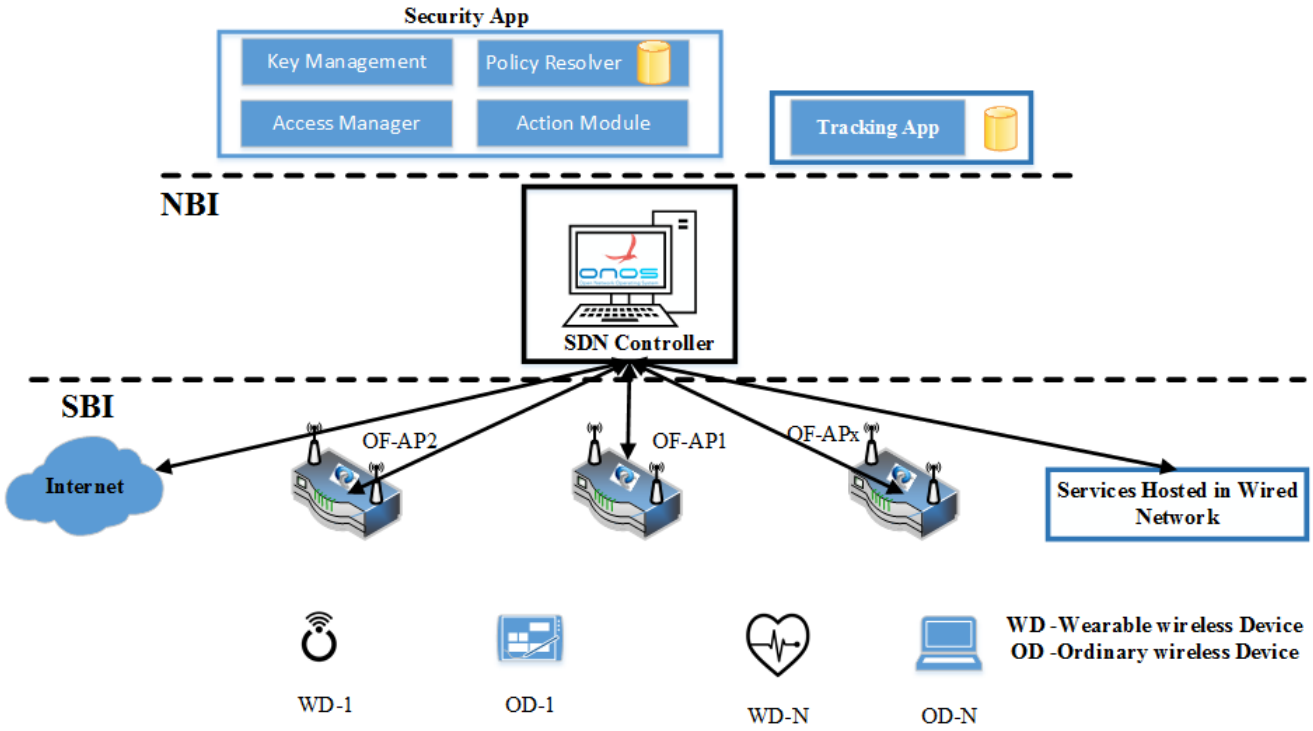

FIGURE 2. SDN monitoring scenario.

Resolver, 3) Key Management Module and 4) Action Module. These components can be implemented on a single server or distributed over several machines. Also the patient tracking component is implemented as a separate application on the SDN Controller.

Access Manager is the Central Management system of the whole Northbound Security System. This Security Application uses a simple language based approach for the specification of the policies. Policies can be specified at fine granular level based on different parameters such as, flow ids, network services, paths, users devices and TCP/IP headers values. A security administrator specifies these policies which are to be enforced in the network domain. The policy terms are stored in a MySQL database. Such a granular specification of policies allows to make the network environment secure [15].

Before explaining the operation of different modules of the Security Application, we first represent how the system works at a high level. When a communication request from the host or devices(Wearable sensor module) arrives at the OpenFlow switch, the switch checks its flow table for matching flow rules. If there is a matching rule then the request is processed according to these policies. If there is no matching rule then the request is forwarded to the SDN Controller. Our Security Application resides at the controller level and is an integral part of the decision-making subsystem of the controller. At this moment Access Manager in Security Application captures the specific details of the new incoming packet, for instance, source IP address, destination IP address, any MAC addresses, port numbers etc. These attributes are passed to the Policy Resolver Module which cross-checks them with

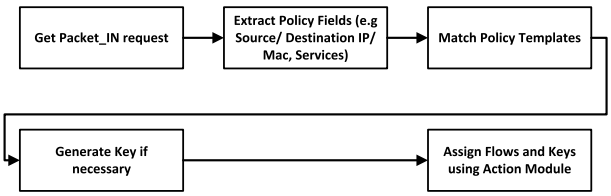

FIGURE 3. Access manager work flow.

the policy templates stored in the MySQL Policy Database. Policy Resolver reports the matching information and actions to the Access Manager. Based on the report Access Manager instructs the Action Module. Action Module updates the OpenFlow switches accordingly by sending Flow_mod messages. We have developed the Security Application in such a way that it only requires minor changes to the Action Module to implement this application with different SDN Controllers.

The other benefit of Security Application is, it is capable of providing on demand confidentiality and integrity services to the user data at the switching layer level. But this feature is dependent on the user or the sensor module. In this case, Access Manager uses Key management module to generate the symmetric keys and Action Module distributes them to pathway switches during communication. Let us now briefly consider the functionalities of the different components of the Security Application:

1) ACCESS MANAGER

The soul of the Security Application is the Access Manager, where all the control logic's reside. The major responsibilities

P_ID	USER	SRC_IP	SRC_MAC	DST_IP	DST_MAC	SERVICES	SEC_PROF	SWITCH_SEQ	PERM
3	Student	*	*	*	*	*	enc	*	P
5	Alice	172.56.16.02	48:2C:6A:1E:59:2F	*	*	*	enc	*	P
6	*	172.56.16.02	48:2C:6A:1E:59:2F	*	*	*	enc	*	P
7	*	*	*	*	*	20,21,22,23	enc	*	P
8	*	*	*	172.56.16.06	56:2D:7F:2E:50:FF	80	enc	*	P
9	*	172.56.16.02	48:2C:6A:1E:59:2F	172.56.16.08	60:FF:2F:D2:60:CC	20,21,22,23	enc	SW1;SW3;SW4	P
10	*	172.56.16.04	48:2C:6A:1E:60:FF	172.56.16.06	56:2D:7F:2E:50:FF	80	enc	SW1;SW5;SW4	P
11	Alice	172.56.16.02	48:2C:6A:1E:59:2F	172.56.16.08	60:FF:2F:D2:60:CC	20,21,22,23	enc	SW1;SW3;SW4	P
12	Alice	*	*	172.56.16.08	60:FF:2F:D2:60:CC	20,21,22,23	enc	SW1;SW2;SW4	P

FIGURE 4. Policy database.

performed by this module are: 1) Packet_in request analysis, 2) Maintain Polices, 3) interact with the Key Management Module, 4) Interact with the Action Module. Flow diagram of the Access Manager is shown in Figure 3.

2) POLICY RESOLVER MODULE

Policy Resolver Module is responsible for maintaining the MySQL database where policies are stored. This Module fetches the particular Policy Templates and sends the report back to the Access Manager.

3) POLICY DATABASE

Policy Templates are stored in the Policy Database. Figure 4 shows a part of the Policy Database. Here, 1) **P_ID** is the policy database id number, 2) **User** is user name, 3) **SRC_IP, SRC_MAC** is the Source IP and MAC addresses respectively, 4) **DST_IP** and **DST_MAC** are the destination IP and MAC addresses, 5) **Service Field** signifies packet type, 6) **SEC_PROF** denotes the security profile, which indicates the security services requested by a user or sensor module such as confidentiality, integrity, authentication services, 7) **Switch_SEQ** is the actual flow path a packet is supposed to take as dictated by the administrator from source to destination.

4) ACTION MODULE

The Action Module is the communication bridge between the Controller and the OpenFlow Switches. This module is responsible for the bidirectional forwarding of messages with Access Manager. Two of the major messages are Packet_IN request and Flow_mod. It also helps to distribute the keys.

D. PATIENT LOCATION MONITORING APPLICATION

The patient location monitoring application tracks the location of the patients and raises alarm for different events such as the location of the patient is violating the policies of the hospital or when the patient is getting to a location that is harmful to the patient. The patient tracking component is implemented as an application on the SDN Controller and on a server in the data plane. To minimise overhead on the SDN Controller, the server in the data plane is used in the default mode of operation for tracking the location of the patients. In case of events such as attacks and congestion in the hospital network, the tracking component on the SDN Controller still ensures the availability of the tracking service.

The Security Application on the SDN Controller ensures that priority is provided to the traffic related to patient tracking application. For example, the Security Application makes use of information such as the global view of the network topology, wearable device ID, total number of devices in the network and traffic originating from the devices to differentiate between the traffic related to patient monitoring application and Internet browsing by the users. Hence when there is congestion, the Security Application dynamically configures the OF-APs to provide priority to the patient monitoring traffic and drop/rate limit other traffic. The wearable devices are configured to send updates to the tracking application at regular intervals (3 seconds in the current implementation). The Action Module in the Security Application configures the OF-APs to forward the updates from wearable devices with high priority. In the current model, the wearable devices are configured to convey only the information of the device ID, Received Signal Strength (RSS) from different OF-APs and battery level available in the device. The device ID enables to identify the patient, the RSS from different OF-APs enables to approximate the location of the wearable device by comparing with the fingerprints stored in the database and the battery level enables to determine if the wearable device has to be replaced with other device.

The location of the patient is determined from the received signal strength from multiple OF-APs at the wearable device. The RSS is the measure of the signal power from the transmitting device to the receiving device. Since there are multiple OF-APs with overlapping range and the location of the OF-APs is fixed within the layout, it is possible to determine the location of wearable device from the RSS. In the training mode, the wearable devices are placed at different locations within the layout and the corresponding RSS from different OF-APs is used to relate the location of at the wearable device in the layout maps and stored in the database. In the online mode, the RSS from different OF-APs at the wearable devices of the patient are compared with the records in the database to approximate the location of patient.

The location tracking database has information on the patients, wearable devices, building layout, signal to location mapping on the layout. The tracking application makes use of the information stored in the database and the RSS of different OF-APs received at the patients wearable device for detecting the current location of the patients with wandering behaviour. Our model makes use of the k-nearest neighbour algorithm to estimate the location of the patients. The k-NN algorithm

computes the Euclidean distances in signal space between the online RSSs and stored RSSs in the database and then calculates the geometrical center of the k-nearest neighbours as the estimated location.

The room allocated to the patient is used as default location for the dementia patient. Mobility of the patient is detected by analysing the changes in the RSS between different OF-APs and the wearable devices. The monitoring application raises high priority alert if the location of dementia patients is found to be moving away from the default location. Hence the nurses and hospital management can track the current location of the patient and take necessary steps to transfer the patient to the default location.

E. ATTACK DETECTION

The attack detection components are used for monitoring the traffic in hospital network and detecting the attacks. The attack detection components can be integrated into the OF-AP's or implemented as additional devices. In this case, the security application configures the routes to ensure that the traffic passes through atleast one attack detection component. The attack detection components makes use of signature and anomaly based techniques for the detection of attacks. For example, it is used to detect attack traffic that is matching with the attack signature and unauthorized SSID broadcast from rouge access points. The attack detection components are configured to raises alarms to the Security Application and /or network administrator if attacks are detected in the network. Furthermore, if unauthorized SSID broadcasts are detected in the network, then the location of rouge access point is approximated by analysing the RSS of the unauthorized SSID. Now let us discuss important sub components that are used for anomaly based detection of the attacks.

Traffic Capture Component(TCC), Traffic Pre-Processing (TPP) and Detection Engine (DE) are the important components for detecting attacks. The first two components are used for capturing the traffic and pre-processing the traffic and the Detection Engine makes use of behavior based intrusion detection approach for detecting the attacks.

1) TRAFFIC CAPTURE COMPONENT

Sniffers are placed at different locations to capture all the communication of the hosts in the hospital network. The TCP/IP header values are used to generate traffic clusters for each end host. The traffic clusters are stored in pcap files which is similar in format to the UNSW-NB dataset [16]. Hence we use the UNSW dataset to validate the performance of attack detection component.

2) TRAFFIC PRE-PROCESSING

The traffic dumps that are captured by the TCC are pre-possessed by converting them into CSV format and feature selection is performed to identify the best features for better performance of the DE. This includes basic features such as source address, destination address, protocol type and other features such as src_bits/sec, number of SYNACK, and dest_bits/sec. The additional features which represent the assosiation between the packet header values are derived by analysing the captured data and stored in CSV format. Now feature selection is performed using recursive feature elimination (RFE) method [17].

3) DETECTION ENGINE

DE is responsible for detecting intrusions in the hospital network. Similar to location detection, there is training mode and testing mode for the detection engine. In training mode, hospital network traffic and different attack traffic is used to train the DE. The profiles in the training mode are used as baseline for detecting the attacks in testing mode. DE uses multiple classifiers and is based on ensemble of Random Forest (RF) and Logistic Regression (LR). RF generates trained multiple decision trees over sub samples of training dataset (bootstrap sample) and presents the output. However one of the issues with RF is that the fully grown trees can lead to over fitting of the training data. So we combine RF with LR module which is used as metaclassifier and then training is performed with the predictions made by RF. The trained classifier is stored in the form of decision model. This trained network intrusion profiles are used as baseline detectors for detecting attacks in the testing mode.

F. DISCUSSION

In this Section, we will provide some discussion related to our model.

- Cost Benefits: The deployment costs are minimal since it makes use of WLAN which is widely deployed in the current networks. Several open sourced and freely available SDN controllers can be used for managing the hospital networks and providing priority to the patient monitoring traffic. There is no need for expensive displays on the wearable devices since our model uses network based tracking of the patients. Hence the cost of wearable devices is also low.Furthermore, the WLAN is efficiently used for continuous monitoring of the patients and also enables other users to access Internet.
- Change of Patient Behaviour: Our model monitors the patient location by analysing the RSS at the wearable devices. The performance of the model is mainly dependent on the training using the wearable devices. Also note that training has to be performed only once to the required level of sensitivity. However the model has to be retrained if there is any change in building layout which is a very rare event. Hence change of patient behaviour does not have any impact on the performance of our model.
- Legitimate failure of the devices: There is a possibility for the failure of the OF-APs and/or the wearable devices. Since the monitoring application has configured the OF-APs to forward the updates with high priority, all the OF-APs that are in the range of the wearable device transmission will forward the update to the monitoring

application. Since the OF-APs are placed with overlapping range, location tracking is still possible in case of failure of the OF-AP. However note that location tracking is not possible in the case of failure of multiple OF-APs in the hospital network. We assume that failure of multiple OF-AP's is a rare event. Failure of the wearable devices will result in absence of the updates from the wearable device to the monitoring application at the expected interval. If the updates are not received for successive intervals, then an alert is raised to the staff with the last known location of the patient.

- Priority for patient monitoring traffic: The traffic related to patient monitoring is differentiated from other traffic based on the wearable device ID and is allocated high priority compared to other traffic. For example, the OF-APs are also used by other patients (without wandering behaviour) and guests of the patients for accessing Internet. Hence in the events such as attacks and congestion, the traffic related to tracking of the patients is given high priority in our model. Now let us consider the case where the OF-APs in critical location receives a request from a wearable device when they are unable to accept any new service requests from a wearable device. Since we assume an overlapping range of the OF-APs the Controller dynamically alters the existing traffic connections from other host machines to different OF-APs and provide priority to the traffic from wearable device. If there are no alternative OF-APs to transfer the traffic from other devices, then the services to other devices are rate limited or terminated to provide priority to the traffic from wearable devices.
- Attacks from user devices: There is a possibility for attacks to be generated from any of the devices in the hospital network. Hence attack detection components are used for monitoring all the traffic in hospital network and detecting the attacks. The attack detection components make use of signature based and anomaly based detection of attacks. In particular, the attack detection monitor for events such as flooding attacks, unauthorized SSID broadcasts from rouge access points and traffic matching with the attack patterns. Also, we make use of behaviour based detection of the attacks. If any traffic from the devices matches with the attack signature or found to be suspicious by the behaviour detection component, then the Security Application dynamically configures the OF-AP to terminate the connections from the malicious host.

IV. IMPLEMENTATION

We have implemented our model with ONOS Controller [18] and OpenFlow based access points as shown in Figure 2.

ONOS [18] adopts a distributed architecture for high availability and scale-out. Many of the modules such as switch manager, module management, link discovery and REST APIs are reused from the Floodlight Controller. Titan graph, Cassandra key value store and the Blueprints graph API

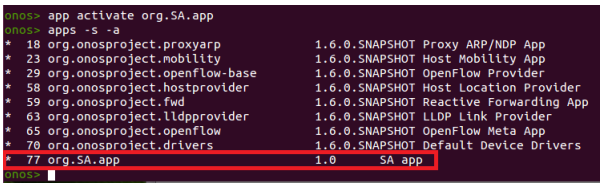

FIGURE 5. Monitoring application for ONOS controller.

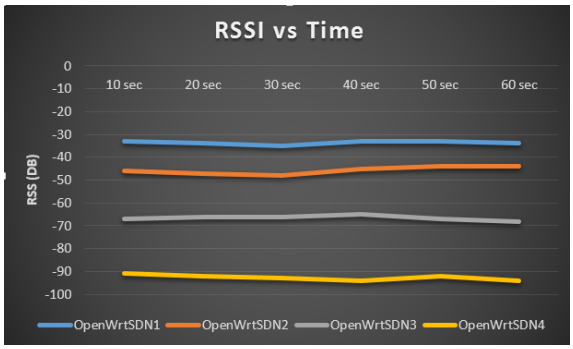

FIGURE 6. RSS vs time.

are used for the implementation of the ONOS data model and exposing the network state to applications. The number of ONOS instances can be varied in accordance with the load. This ensures high availability of the controller. In the case of distributed implementation, each Controller instance maintains the global network view but maintains part of the network. Hence applications hosted on any instance of the controller can still make use of the global information of the network available at the Controller to make forwarding and policy decisions and write their policies to be enforced on the network view. Any changes in the policy are sent to the corresponding manager for enforcement of policies on the appropriate switches.

OpenFlow Wireless APs are not commercially available. For this reason, we have developed our own OpenFlow wireless AP using TP-link (TL-WR1043ND) wireless AP since they are low cost, easily available, and customizable. We have installed Open vSwitch to make the device compatible to OpenFlow 1.3. First we have replaced the old firmware of TL-WR1043ND with OpenWrt [19]. OpenWrt uses linux kernel (2.6) and was mainly used in embedded devices for instance ARM, Raspberry, some commercial and Customized APs for network traffic routing. Then installed and configured Open vSwitch to make the OpenWrt, OpenFlow enabled. This creates provision for connecting remote host wirelessly using OpenFlow.

As shown in Figure 5, we have developed Security Application for ONOS SDN Controller to enforce fine granular policies for communication between the hosts.

We have developed our own tracking device using Arduino uno, ESP8266 and a voltage regulator IC. The purpose of the device is to send the RSS value of nearby OF-APs to the location tracking application. We have used a 6000mAH

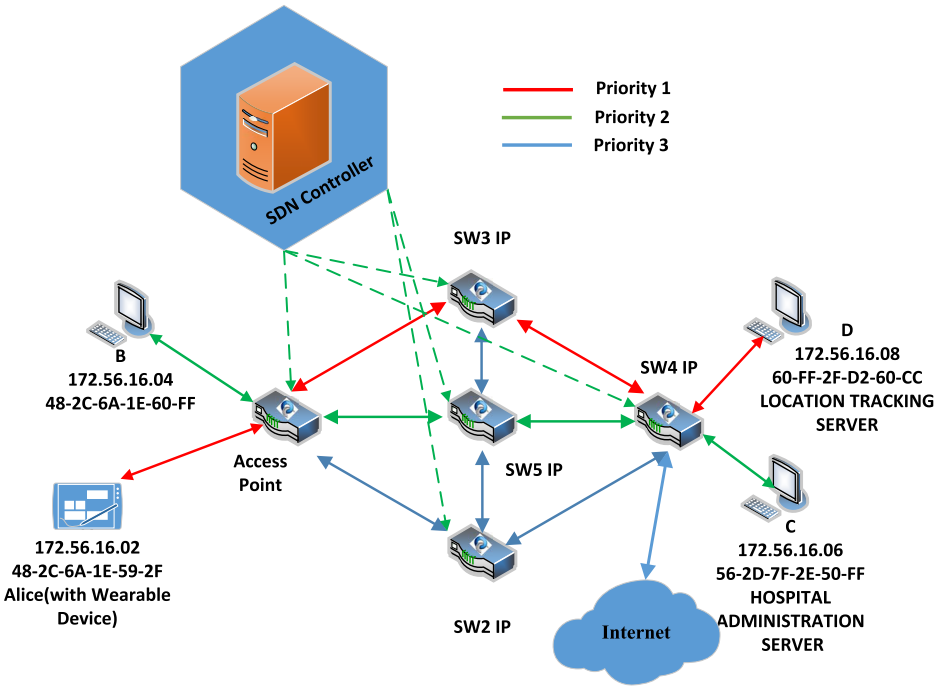

FIGURE 7. Priority based access to services.

5volt battery to power the whole unit. This arrangement is extremely light weight and consumes less power (sufficient for powering the unit for more than one day). Arduino uno is a Micro-controller programmable interface that can be used for making small IoT units. ESP8266 is a very famous miniature WLAN chip which provides wireless capability to the Arduino. Since, ESP8266 (3.3V) works in a lower voltage than the Arduino, we have used a voltage regulator IC(1117). Arduino maintains a serial communication with ESP8266 and our chosen baud rate in this case is 9600. One of the I/O pin in Arduino is programmed to sense the battery level. Figure 6 shows a trace of RSS from different SDN OF-APs in a particular time and from a particular tracking device.

A. PRIORITY BASED ACCESS TO SERVICES

In this section we will describe how our Security Application provides priority services to the patient tracking services. Figure 7 shows the case where a patient with wearable device and staff member is accessing different services from the same OF-AP. Also the staff member is using his wireless device to access some administrative service in the wired network in the hospital and access some services in the Internet. In this scenarios, the aim of the Security Application is to provide high priority to the traffic from the wearable device, second priority to the staff wireless device for accessing administrative services hosted in the wired network and low priority to staff wireless device for accessing Internet. When the flows are initiated by the devices, the Security Application extracts the Source ID, Destination ID and makes use of the policy resolver for determining the related policies. Since the administrator configured policies to provide high priority to the traffic from wearable device to the tracking application, it receives high priority. Then the traffic from the staff device which is destined to the server with administrative services receives second priority. Finally the traffic destined to the Internet receives lowest priority.

B. PATIENT TRACKING

The whole implementation setup was created in our research labs. We have used the whole third floor of our University building to test and train the model with a sample hospital setup.

For this prototype setup, we have used two type of devices. One is a custom made patient tracking hardware. This uses Arduino Uno board to mount the sensor and maintain communication with the OF-AP. The other one is a traditional Samsung Mobile with an RSS recording android application in it.

In Figure 8 we have marked the position of the OF-AP(OpenWrtSDNX) using green stars. The RSS variations are recorded by the custom devices. Based on the RSS strength from OF-AP's, the sensor locations/ patient location/ mobility of patients are detected. In most of the cases, the devices are connected to the OF-AP with highest RSS strength. But in some severe cases where OF-AP signals are obstructed and becomes faulty, signal strength can fall significantly. In those cases, Security Application assigns an alternative OF-AP to the wearable device. The wireless devices are connected to the neighbouring OF-APs if the signal strength is at least 20 percent greater than the

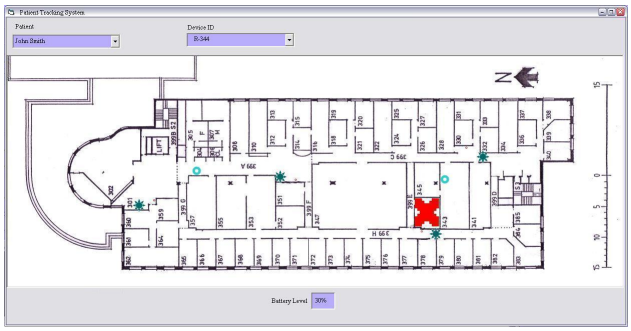

FIGURE 8. Patient location.

signal strength of the current OF-AP. In the case of congestion of specific OF-APs, the wearable devices are given high priority for connecting to the default OF-APs. Other client devices are redirected to the OF-APs with minimal load.

First, we captured random RSS and location data to train the model. The RSS values and location information are stored in a SQL database, which is used for this training purpose. We have taken fifteen training samples for default location of the patients and 10 samples for other locations. They are grouped into two categories based on the patient's probable location in the room. A major percentage of the patients location will be close to the bed. So we have collected fifteen samples at different locations on the bed such as corners of the bed, center of the bed. Then 10 samples are taken from different locations such as toilet, fridge and room entry. Then we have tested the model by placing custom wearable devices in different locations in the floor layout. The model achieved accuracy of 2 feet for the locations with 15 training samples and 1 meter accuracy for the cases with 10 training samples.

The graphical interface to track the patient's location is illustrated in Figure 8. OF-APs and attack detection components are represented by the stars and blue circles respectively. The attack detection components are used for the detection of network attacks, unauthorized SSID broadcasts from rogue access points. Patient names and/or device ID are used to query for the the location of patients. The application graphical interface also displays the power level of the wearable device. Our current model raises different priority alerts for the following events :

- **High alert events:** patient moving away from the default location(allocated room); patient entering into rooms of other patients; patient moving towards exit gate of the hospital, attacks detected in hospital network traffic; when the battery level on the wearable device is at 10 percent; when signals from wearable devices are not received for four successive intervals.
- **Medium alert events:** when the traffic exceeds maximum threshold in hospital networks; when the battery level on the wearable device is at 20 percent, when signals from wearable devices are not received for three successive intervals;

TABLE 1. Evaluation metrics and their description.

Parameter	Description
True Positive (TP)	IDS detects the intrusive program execution as malicious
False Positive (FP)	IDS detects the normal execution of the system as malicious
True Negative (TN)	IDS detects the normal program execution as normal
False Positive (FN)	IDS detects the intrusive program execution as normal
Accuracy	(TN + TP)/(TN + TP + FN + FP); It describes the degree to which an algorithm can correctly predict the positive and negative instances.
FPR	FP/(TN+FP); The proportion of incorrectly classified intrusions to the actual size of the attack class

TABLE 2. Performance results over UNSW-NB intrusion dataset.

Classifiers	Accuracy (%)	False Positive Rate (%)
RF	86.67	2.815
GBT	94.12	6.23
RT+LR	92.311	2.70
RF+LR	94.54	2.81
DT [16]	85.56	15.78
NB [16]	82.07	18.56
LR [16]	83.15	18.48
ANN [16]	81.34	21.13
EM clustering [16]	78.47	23.79

- **Low alert events:** when the battery level on the wearable device is at 30 percent, when signals from wearable devices are not received for two successive intervals;

C. ATTACK DETECTION ANALYSIS

We have evaluated the attack detection performance using the UNSW-NB [16] dataset. The dataset contains 47 features and 10 different types of attacks such as rootkits, fuzzers, shellcode and worms. More details on the dataset are available at [20]. Table 1 shows different parameters that are used for the evaluation of traffic monitoring functionality. We have used feature selection for better performance of the classifiers. The dataset is processed and fine tuned with the classifier by transforming the features, normalizing and scaling the dataset. We have considered different ensemble classifiers such as Random Trees Embedding Classifier (RT), Gradient Boosting Classifier (GB) and RF Classifier to improve the results of single classifier algorithms and LR [21] was used as a meta estimator to combine the predictions of different learners using RF. Finally we have obtained total of 16 features {dstip, dsport,dmeansz, dload, srcip, sbytes, sttl, sload, smeansz, stime, ltime, tcprtt, ct_state_ttl, ct_flw_http_mthd, ct_srv_src, ct_srv_dst } by using RF recursive feature elimination method.

We have developed an ensemble method to achieve better performance compared to Moustafa and Slay [16] which has used only single classifiers. From table 2, it is clear that all our ensemble classifiers provide better performance compared to the results achieved by [16] using different single classifiers. Since RF + LR provides best performance compared to all other ensemble classifiers, we have used this classifier with 16 features for training the DE.

V. RELATED WORK

In this section, we present some of the related work in the areas of localisation techniques, attacks in WLAN and SDN security.

Techniques such as [22]–[25] have been proposed earlier for tracking the location in outdoor and indoor environments. For example, GPS based tracking [22] techniques provide an accurate location estimation in the areas where there is a line-of-sight from the satellites to the tracked device. Hence it is mostly used in open environments. However, it is not efficient for location tracking inside buildings due to signal blockage by walls and multipath effects. Hence we need to make use of indoor location tracking techniques such as [23]–[25] for monitoring the location of patients. However we also need to consider different requirements such as the deployment cost of the devices, operational costs of the technology, training of the non technical staff for using the technology and providing priority for the patient monitoring application.

There are several prior works related to security in wireless networks. Some of the work has considered different possible attacks [26]–[31] in wireless networks. For example, Khan et al [26] presented the challenges to deal with the passive attacks in wireless networks and [27], [29], [30] demonstrated different types of denial of service attacks that are possible in such networks. Also techniques have been proposed [31]–[36] to deal with some of the attacks in such networks. For example, techniques have been proposed to deal with the denial of service attacks using MAC and traffic pattern filtering [32] and active queue management [34] to deal with the flooding attacks, using cookies to provide access to authenticated devices [33], and dynamic variation of the communication channel [31] to complicate jamming attacks. Also, [35] and [36] proposed techniques to detect rouge access points in networks. Reference [35] proposed to make use of USB adapters for monitoring network to detect SSID broadcast messages from rouge access points. Reference [36] proposed to detect rouge access points by analyzing the time delays between the communication of mobile devices and local servers. There is a need to consider such wireless attacks and solutions in the design of secure healthcare applications.

SDN is still relatively new technology and there is ongoing debate [37], [38] on the advantages and concerns with this technology. It can take considerable time to realise the benefits and additional threats with the technology. Some of the work has considered different possible attacks [39]–[41] related to the technology and work such as [12]–[14] and [42] has focused on securing the SDN networks. Our wok mainly makes use of the innovation in SDN to address the specific issues related to healthcare applications.

The current paper is an extend version of the paper [43]. Earlier we have also proposed techniques [44] for monitoring dementia patients without SDN. However location tracking without SDN cannot efficiently handle the dynamic changes in networks resulting due to events such as legitimate failure of devices, congestion and attacks. We have also developed policy based application [15] for SDN Controllers without considering the specific requirements of healthcare applications (such as location tracking of the patients) and also used machine learning techniques for detection of attacks [45] in cloud environments with virtual systems. However there is need for real time location tracking of the patients with wandering behaviour and detect attacks in networks with several other wireless and wired devices. Hence the current submission aims to address the specific issues related to monitoring patients by making use of machine learning techniques and SDN for tracking the location of patients, efficiently handle the dynamic changes in networks and deal with the attacks to provide priority to the traffic related to patient monitoring.

VI. CONCLUSION

In this paper we have proposed techniques for making use of the SDN for secure and real time monitoring of the patients with wandering behaviour in hospital environments. We discussed how SDN can help to resolve some of the challenges for real time location monitoring of the patients and offers advantages for such critical applications. Since an SDN Controller has a global view of the network, devices in the network and traffic originating from the devices, our model makes use of this information to differentiate between the traffic related to patient monitoring application and Internet browsing by the users. Hence in events such as congestion, legitimate failure of devices and attacks, the Controller dynamically configures the OpenFlow Access Points (OF-APs) to provide priority to the patient monitoring traffic and drop or rate limit other traffic.We have also presented a prototype implementation of our model using ONOS SDN Controller and OpenFlow access points.

REFERENCES

[1] *What is Dementia?* Accessed: Jul. 6, 2017. [Online]. Available: http://www.alz.org/what-is-dementia.asp
[2] P. Dawson and D. W. Reid, "Behavioral dimensions of patients at risk of wandering," *Gerontologist*, vol. 27, no. 1, pp. 104–107, 1987.
[3] C. K. Y. Lai and D. G. Arthur, "Wandering behaviour in people with dementia," *J. Adv. Nursing*, vol. 44, no. 2, pp. 173–182, 2003.
[4] D. L. Algase, E. R. A. Beattie, and B. Therrien, "Impact of cognitive impairment on wandering behavior," *Western J. Nursing Res.*, vol. 23, no. 3, pp. 283–295, 2001.
[5] C. Iadecola, "The pathobiology of vascular dementia," *Neuron*, vol. 80, no. 4, pp. 844–866, 2013.
[6] B. Jordan. (2013). *Emergency Services Find Lost Dementia Sufferer*. [Online]. Available: http://www.greatfete.com.au/media/NewsLocal-HillsShireTimes-13Aug2013-Page3.pdf
[7] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.
[8] M. Alhussein, "Monitoring Parkinson's disease in smart cities," *IEEE Access*, vol. 5, pp. 19835–19841, 2017.
[9] M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, "Disease prediction by machine learning over big data from healthcare communities," *IEEE Access*, vol. 5, pp. 8869–8879, 2017.
[10] O. N. Foundation. *Software-Defined Networking: The New Norm for Networks*. Accessed: Dec. 12, 2015. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdnresources/white-papers/wp-sdn-newnorm.pdf
[11] A. Shalimov, D. Zuikov, D. Zimarina, V. Pashkov, and R. Smeliansky, "Advanced study of SDN/openflow controllers," in *Proc. ACM 9th Central Eastern Eur. Softw. Eng. Conf. Russia*, 2013, p. 1.

[12] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for openflow networks," in *Proc. ACM 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 121–126.

[13] H. Li, P. Li, S. Guo, and S. Yu, "Byzantine-resilient secure software-defined networks with multiple controllers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 695–700.

[14] S. Shin *et al.*, "Rosemary: A robust, secure, and high-performance network operating system," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 78–89.

[15] K. K. Karmakar, V. Varadharajan, U. Tupakula, and M. Hitchens, "Policy based security architecture for software defined networks," in *Proc. 31st Annu. ACM Symp. Appl. Comput. (SAC)*, New York, NY, USA, 2016, pp. 658–663. [Online]. Available: http://doi.acm.org/10.1145/2851613.2851728

[16] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. IEEE Military Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.

[17] I. Guyon, S. Gunn, M. Nikravesh, and L. A. Zadeh, *Feature Extraction: Foundations and Applications*, vol. 207. Stone Harbor, NJ, USA: Springer, 2008.

[18] P. Berde *et al.*, "Connor, P. Radoslavov, W. Snow, "ONOS: Towards an open, distributed SDN OS," in *Proc. ACM 3rd Workshop Hot Topics Softw. Defined Netw.*, 2014, pp. 1–6.

[19] *OpenWrt*. Accessed: Jul. 6, 2017. [Online]. Available: https://openwrt.org/

[20] ACCS. (2015). *The UNSW-NB15 Data Set Description*. [Online]. Available: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/cybersecurity/ADFA-NB15-Datasets/

[21] D. W. Hosmer, Jr., and S. Lemeshow, *Applied Logistic Regression*. Hoboken, NJ, USA: Wiley, 2004.

[22] P. Enge and P. Misra, "Special issue on global positioning system," *Proc. IEEE*, vol. 87, no. 1, pp. 3–15, Jan. 1999.

[23] A. Agiwal, P. Khandpur, and H. Saran, "Locator: Location estimation system for wireless lans," in *Proc. 2nd ACM Int. Workshop Wireless Mobile Appl. Services WLAN Hotspots*, 2004, pp. 102–109.

[24] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. IEEE 19th Annu. Joint Conf. Comput. Commun. Soc. (INFOCOM)*, vol. 2. Mar. 2000, pp. 775–784.

[25] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, and X. Gao, "A wireless LAN-based indoor positioning technology," *IBM J. Res. Develop.*, vol. 48, nos. 5–6, pp. 617–626, 2004.

[26] S. Khan, K.-K. Loo, T. Naeem, and M. A. Khan, "Denial of service attacks and challenges in broadband wireless networks," *Int. J. Comput. Sci. Netw. Secur.*, vol. 8, no. 7, pp. 1–6, 2008.

[27] J. Bellardo and S. Savage, "Denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX Secur.*, 2003, pp. 15–28.

[28] C. He and J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," in *Proc. 12th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2005, pp. 90–110.

[29] R. H. Rahman, N. Nowsheen, M. A. Khan, and A. H. Khan, "Wireless LAN security: An in-depth study of the threats and vulnerabilities," *Asian J. Inf. Technol.*, vol. 6, no. 4, pp. 441–446, 2007.

[30] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, "Vulnerabilities of wireless security protocols (WEP and WPA2)," *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)*, vol. 1, no. 2, pp. 34–38, 2012.

[31] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proc. 3rd ACM Workshop Wireless Secur.*, 2004, pp. 80–89.

[32] C. Liu and J. Yu, "A solution to WLAN authentication and association DOS attacks," *IAENG Int. J. Comput. Sci.*, vol. 34, no. 1, pp. 31–36, 2007.

[33] R. Zeng, C. Lin, H. Yang, Y. Wang, Y. Wang, and P. Ungsunan, "A novel cookie-based DDoS protection scheme and its performance analysis," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, May 2009, pp. 861–867.

[34] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 40–53, Feb. 2009.

[35] P. Bahl *et al.*, "Enhancing the security of corporate Wi-Fi networks using DAIR," in *Proc. ACM 4th Int. Conf. Mobile Syst., Appl. Services*, 2006, pp. 1–14.

[36] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912–1925, Nov. 2011.

[37] L. Schehlmann, S. Abt, and H. Baier, "Blessing or curse? Revisiting security aspects of software-defined networking," in *Proc. IEEE 10th Int. Conf. Netw. Service Manage. (CNSM) Workshop*, Nov. 2014, pp. 382–387.

[38] M. C. Dacier, H. König, R. Cwalinski, F. Kargl, and S. Dietrich, "Security challenges and opportunities of software-defined networking," *IEEE Security Privacy*, vol. 15, no. 2, pp. 96–100, Mar./Apr. 2017.

[39] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 55–60.

[40] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures," in *Proc. NDSS*, 2015, pp. 1–15.

[41] S. Lee, C. Yoon, C. Lee, S. Shin, V. Yegneswaran, and P. Porras, "DELTA: A security assessment framework for software-defined networks," in *Proc. NDSS*, vol. 17. 2017, pp. 1–15.

[42] A. Dixit, F. Hao, S. Mukherjee, T. V. Lakshman, and R. R. Kompella, "ElastiCon; an elastic distributed SDN controller," in *Proc. 10th ACM/IEEE Symp. Archit. Netw. Commun. Syst.*, Oct. 2014, pp. 17–28.

[43] U. Tupakula, V. Varadharajan, and K. Karmakar, "Secure monitoring of the patients with wandering behaviour," in *Proc. 11th EAI Int. Conf. Body Area Netw. (ICST)*, 2016, pp. 111–117. [Online]. Available: http://dl.acm.org/citation.cfm?id=3068615.3068641

[44] U. Tupakula and V. Varadharajan, "Secure monitoring for dementia patients," in *Proc. 29th Annu. ACM Symp. Appl. Comput.*, 2014, pp. 14–19.

[45] P. Mishra, E. S. Pilli, V. Varadharajant, and U. Tupakula, "NvCloudIDS: A security architecture to detect intrusions at network and virtualization layer in cloud environment," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2016, pp. 56–62.

VIJAY VARADHARAJAN is currently a Global Innovation Chair Professor of cyber security with The University of Newcastle. He is also the Director of the Advanced Cyber Security Engineering Research Centre. He has published over 400 papers in international journals and conferences. He has been on the Editorial Board of several journals, including the ACM TISSEC, the IEEE TDSC, the IEEE TIFS, and the IEEE TCC.

UDAY TUPAKULA received the Ph.D. degree in computing in 2006 under the supervision of Prof. Varadharajan. He is currently a Senior Lecturer of cyber security with The University of Newcastle. He is also a member of the Advanced Cyber Security Engineering Research Centre. He has 70 publications in different research areas, such as network security, denial of service attacks, MANET security, and secure virtual systems.

KALLOL KARMAKAR is currently pursuing the Ph.D. degree in computer engineering with the Advanced Cyber Security Research Centre, Macquarie University. He is involved in software defined network security.