Secure Monitoring of the Patients with Wandering Behaviour

Udaya Tupakula, Vijay Varadharajan, Kallol Karmakar
Advanced Cyber Security Research Centre
Faculty of Science, Macquarie University
Sydney, Australia
{udaya.tupakula, vijay.varadharajan}@mq.edu.au,
Kallol.Karmakar@students.mq.edu.au

ABSTRACT

Today there are several health care related problems such as dementia and cancer with no possible cure. Hence there is considerable interest in the medical sectors and constant encouragement from the governments to make use of the latest technological advancements for supporting such patients. Software Defined Networking(SDN) is a promising technological advancement in the networking world. In this paper we propose techniques for making use of the SDN, Wireless LAN and wearable devices for secure monitoring of the patients with wandering behaviour in hospital environments. Our model makes use of the global network knowledge available at the SDN controller to deal with the attacks in WLAN and provide priority for real time location monitoring of the patients. We will also present the prototype implementation of our model using ONOS SDN controller and OpenFlow Access Points.

CCS Concepts

•Security and privacy → Usability in security and privacy;

Keywords

Secure Healthcare, Dementia, Wandering, SDN, Security attacks, WLAN Localisation, SDN, OpenFlow

1. INTRODUCTION

Dementia [1, 9, 17, 4] causes degradation of mental ability to a level that can interfere with the tasks performed in daily life. There are different forms of dementia such as Alzheimer's, vascular dementia, Parkinson's disease dementia and mixed dementia. Although this is more common in aged people, there are cases where young people are infected with such disease. Currently there is no cure for some forms of dementia and the life span of the patients can range from 5-20 years depending on the seriousness of disease. Alzheimer's is one of the most common forms of dementia which is followed by vascular dementia which occurs after a stroke. Vascular dementia results due to blockage of major blood vessels in the brain and can severely impact the mental ability of the patient. Depending on the damage of the blood vessels the patient can have symptoms such as confusion, vision loss, wandering, trouble with speaking and understanding.

There are several challenges for the hospitals to deal with patients with specific requirements such as patients with vascular dementia. For example, vascular dementia patients who have been admitted to hospital after stroke for treatment can exhibit behaviour that is harmful for the patient and also violate policies of the hospital. In some cases, dementia patients can get into some locations that is harmful for them and will not be able to convey any information due to the conditions caused by the vascular dementia. In some cases, the vascular dementia patients can enter the room of other patients and violate their privacy. In some cases, the dementia patients can leave the hospital premises. For example, [14] reported a case of missing dementia patient from Anglican Care Nursing Home at Castle Hill, Sydney. Failure to detect such events is serious concern for hospital managements. Hence, even minor lack of attention from the nursing staff can lead to havoc or security breach in such environments. Although the nursing staff make sincere effort for taking care and monitoring of the patients, it is rare that a nursing staff is allocated to each patient. Hence there is a need for continuous location monitoring for some of the patients with specific requirements such as people with vascular dementia.

Currently there is considerable interest for making use of different heterogeneous technologies for healthcare applications. 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 environ-

BODYNETS 2016, December 15-16, Turin, Italy

DOI 10.4108/eai.15-12-2016.2267665

ment. One of the aims of our work is to use technology for secure monitoring of vascular dementia patients from getting into locations that are harmful to the patient or detect if the behaviour of the patient violates the policies of the hospital, or even violates privacy policies of other patients. Our approach makes use of Software Defined Networks(SDN), Wireless LAN (WLAN) and wearable devices of 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 Internet and the open nature of the communication 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. For example, since a SDN Controller has a global view of the network, devices in the network and traffic originating from the devices, it is able to differentiate between the traffic related to patient monitoring application and Internet browsing by the users. Hence in events such as congestion, the Controller can dynamically configure the OpenFlow Access Points(OF-APs) to provide priority to the patient monitoring traffic and drop/rate limit other traffic.
The paper is organised as follows. Section 2 gives a brief overview of the SDN technology and Section 3 presents some of the related work. In Section 4, we present our approach and operation of our model. Section 5 presents the implementation details and Section 6 concludes.

2. SDN OVERVIEW

SDN [11] enables programmable networks and simplifies the tasks of the network administrators for managing complex networks. The idea of SDN is based upon the separation of the control plane from the data plane. This separation results in the network switches becoming simpler forwarding devices with the control logic implemented in a logically centralized Controller. Also, it enables the design of new innovative network functions, protocols and applications. First, it is simpler and less error-prone to modify network policies through software, than via low-level device configurations. Second, a control program can automatically react to spurious changes of the network state and thus maintain up to date high-level policies in place. Third, the centralization of the control logic in the Controller with network wide knowledge simplifies the development of more sophisticated network functions.

Figure 1 shows an overview of the SDN architecture with different components in the control plane and data plane. The control plane consists of a logically centralised Controller (which can be distributed in practice) with native applications for the management and security (rarely considered by existing Controllers) of the devices in SDN network. Also there can be several 3rd party applications that can be hosted or accessing different services in the Controller. The interface between the Controller and the applications is called as the North Bound. The data plane consists of the networking devices and the interface between the Controller and the networking devices is called as the South Bound. OpenFlow [11] is one of the commonly used protocols for communication between the Controller and the networking devices. However different protocols such as sflow, and snmp are also supported for communication between the

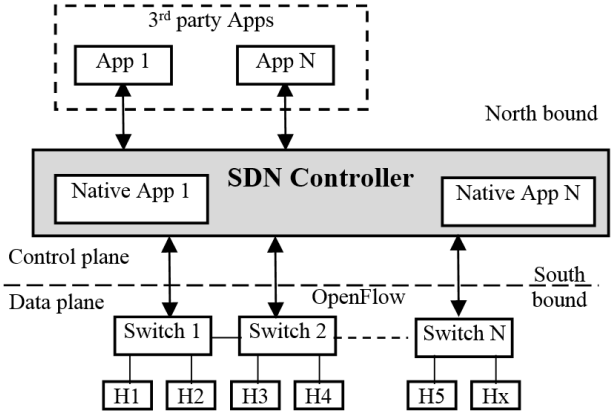

Figure 1: SDN Overview

Controller and the switches. In SDN terminology, a switch is used to represent any networking device that operates in Layers 2 to 7 in the OSI model.
The Controller manages the flow-entries in the flow tables of the switches through a secure channel (that exists in the switch itself). This management process might be done both reactively (in response to packets) as well as proactively. There are several SDN Controllers [22] available at present with different programming languages and environments. For example, NOX is based on C++ and Python programming languages; POX is based on Python; and Beacon and Floodlight are based on Java.
An OpenFlow compatible switch in the data plane contains three parts: i) A flow table, with an action linked with each flow entry, which tells the switch how to process the flow; ii) A secure channel that joins a switch to a remote control process (the Controller), allowing instructions and packets to be sent between a Controller and the switch using OpenFlow protocol; iii) The OpenFlow protocol, which provides an open and standard way for a Controller to interconnect with a switch. An entry in the flow table has three fields: a) a packet header that defines the flow; b) the action, which defines how the packets should be handled; c) counters, which keep track of the amount of packets per flow, and the time since the last packet matched the flow.
In traditional networks, when the network devices receive the traffic from the host, they make a decision depending on the route information available in the device (configured using CLI and/or captured from different network devices) and destination address of the traffic. In SDN, the OpenFlow switches are only used as dumb devices. When the switches receive a flow from a host, they simply forward the traffic as packet in messages to the Controller and rely on it to establish the communication path. Since the Controller has a global view of the network, it makes a dynamic decision on how to forward the traffic to the destination and configures corresponding flow rules on all the switches between the source and destination. 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.

3. RELATED WORK

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

Different location tracking techniques [10, 3, 6, 25] have been proposed earlier. For example, GPS based tracking [10] 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. Techniques such as [3, 6, 25] can be used for indoor tracking but we need to consider the special requirements for dementia patients. For example, during the events such as congestion, there is a need to provide priority for the traffic related to patient monitoring. Also, there is a need to deal with the attacks originating in the wireless networks.

There are several prior works related to the attacks, analysis of the security protocols that have been proposed for secure communication in wireless networks and techniques to deal with the attacks in wireless networks. For example, Khan et al [15] considers different types of attacks that are possible in the WLAN, WiMax and WMAN technologies. The work specifically highlights the challenges to deal with the passive attacks and categorization of attacks at different layers of the protocol stack. Bellardo and Savage [7] have demonstrated how the attacker can perform different types of denial of service attacks such as deauthentication and disassociation attacks. He and Mitchell [13] also observed DoS vulnerabilities in 802.11i and the work in [21, 16] presents a detailed discussion on how the attacks can be implemented in practice. Liu and Yu [19] analyzed the authentication request flooding and association request flooding attacks and proposed to use MAC address filtering and traffic pattern filtering which enforces a limit on the maximum number of authentication or association requests from the mobile nodes. Furthermore, some techniques have been proposed to deal with the rogue access points in the wireless networks. Bahl et al [5] suggested dense deployment of sensors for monitoring the wireless networks for rouge access points. The technique makes use of the unused desktop resources in wired networks and USB based wireless adapters to minimize the deployment cost of the security sensors. The techniques proposed by Sheng et al [12] can be used to detect if mobile devices are connected to rouge access points. Since a wireless rogue access point can induce time delays between the communications, [12] detect the rouge access points by monitoring the changes in the round trip time when communicating with the local servers. Zeng et. al [27] proposed cookie based approach to deal with the denial of service attacks on the authentication mechanism during handover process. Xu et al [26] considered different types of jamming attacks and proposed dynamic changing of communication channels to deal with the attacks. Traynor et. al [24] used queue management techniques to deal with the saturation of the wireless links. Compared to these related work, our work addresses the specific requirements for secure healthcare applications particularly for dementia patients and makes use of SDN to deal with the attacks in WLAN.

There is some prior work related to security in SDN. Porras et al. [20] discussed the security challenges and the need for security enforcement kernel at the Controller. They proposed a role based enforcement of security policies and conflict resolution for NOX Controller. Li et al. [18] proposed to use multiple Controllers to deal with the case of failure or compromise of single Controller and each switch is managed by more than one Controller. To protect SDN from such kind of threats to the control plane, this technique assumes that majority of the Controllers are not compromised by the attacker and deals with the challenge of letting the Controllers continue operate correctly, even if some of them exhibit arbitrary, possibly malicious behavior. Shin et al. [23] proposed ROSEMARY to improve the resilience of the SDN Controller. Its design is based on sandboxing the network applications to prevent common failures of network applications from halting the SDN Controller operation. The main focus of our work is to make use of SDN to address some of the challenges related to secure and real time monitoring of the patients in hospital environment. Furthermore the proposed techniques [20, 18, 23] can complement our model for improving the security in SDN. For example, since the Controller has several 3rd party applications, role based access control can be enforced at the Controller in our model (similar to [20]) to deal with the malicious 3rd party applications and conflict resolution of the policies. Similarly multiple Controllers (such as [18]) or sandboxing of network applications in the Controller [23] can be used in our model to deal with the failure or compromise of the Controller.

4. 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.

4.1 Requirements

- Although there is a need for continuous location monitoring of the dementia patients, 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. Hence it is advantageous for making use of the widely deployed technologies such as WLAN.
- 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 it is more useful for the nurses and hospital management to keep track of the dementia patients.
- The wearable devices are initially used to train our model for detecting the location of device to the re-

quired level of accuracy. As the number of samples used for training our model increase, the location detection accuracy of our model increases. Note that change in the layout of the building is somewhat a rare event, the training has to be performed only once to the required level of sensitivity. In case of changes to the building layout, the training data has to be updated to track the locations in the new layout.

- Patients with dementia can change their behavior. However this does not have any impact on our model since its operation is dependent only on the training using the wearable device.
- 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. 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.

4.2 Operation

As shown in the Figure 2, we consider a scenario where SDN is used for managing the WLAN. The WLAN is used for real time monitoring of the dementia patients and also for providing Internet services to other users (patients without dementia, guests and hospital staff). OF-APs are placed at different locations within the layout with overlapping range and there are some wireless sniffers (not shown) to capture the traffic in WLAN and monitoring 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 [20, 18, 23] can be used for security and high availability of the Controller.

As shown in the Figure 2, we have developed a secure monitoring application for ONOS Controller for real time location tracking of the patients with wandering behaviour and deal with the attacks in WLAN. The monitoring application tracks the location of the patients and raises alarms to the hospital staff when the location of the dementia patient is violating the policies of the hospital or when the battery power in the wearable devices is falling below a threshold for recharging the devices. The monitoring application can be installed on any of the SDN Controllers with minimal modification. The application makes use of the global network information available at the SDN Controller and has additional sub components to provide priority to the traffic related to the patient monitoring and also deal with the attacks in WLAN. For example, the monitoring application makes use of information such as the global view of the network topology, devices in the network and traffic originating

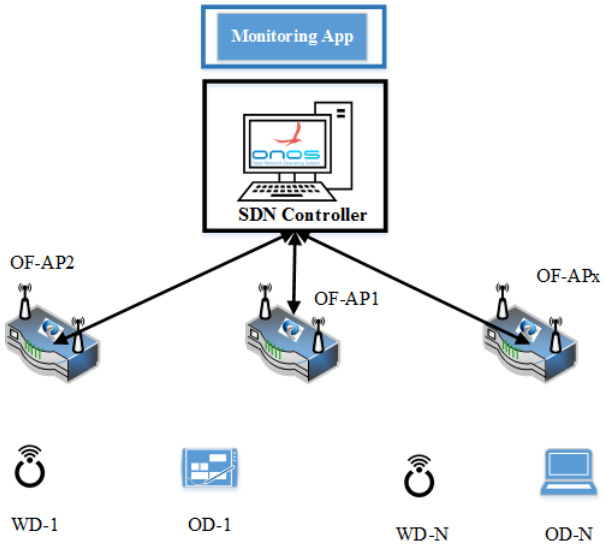

Figure 2: SDN Monitoring Scenario

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 Controller can dynamically configure 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 monitoring application at regular intervals (3 seconds in the current implementation). Also the monitoring 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 monitoring system has different sub components such as authentication, attack detection, database, and location tracking. Our current implementation makes use of shared secret and also supports 802.11i security. A detailed analysis

of the 802.11i security can be found in [13]. Attack detection is based on signature matching, unauthorized SSID broadcast, and monitoring of the time delays between the transmitted and received signals. The signals transmitted from the wearable devices and OF-APs are time stamped just before transmission to discourage attacks. For example, the round trip time between the wearable devices and the OF-APs is used to detect man in the middle attacks. A detailed analysis on detecting such attacks can be found in [12]. If there is considerable delay between the signal transmitted by wearable device and signal received at the OF-AP then this can be considered to be suspicious. In such cases, our model raises alarms to the network administrator for physical monitoring of the location. Furthermore, if the sniffers detect any unauthorized SSID broadcasts, then RSS of the unauthorized SSID is also used to approximate the location of malicious devices. The database has information on the patients, wearable devices, building layout, signal to location mapping on the layout. The location monitor component makes use of the information stored in the database and the RSS for detecting the current location of the dementia patients. 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.

4.3 Discussion

In this Section, we will provide some discussion related to 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. To deal with the failure of the OF-AP, the Controller configures atleast two OF-APs to forward the traffic from wearable device to the monitoring application. 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 dementia) 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 other user devices: There is a possibility for attacks to be generated from other hosts that are making use of WLAN for accessing Internet. Hence all the traffic received at the OF-APs is monitored using the signature based detection engine. Furthermore, the sniffers capture all the traffic in the wireless medium and monitor for events such as congestion, unauthorized SSID broadcasts from rouge access points and also match the captured traffic with the known attacks signatures to detect if there is any ongoing attack. If any traffic from the other devices matches with the attack signature, then the monitoring application determines the OF-AP that is connected to the malicious host and dynamically configures the OF-AP to terminate the connections from the malicious host.

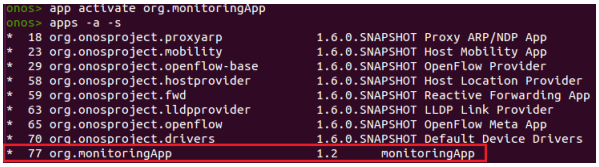

Figure 3: Monitoring Application for ONOS Controller

5. IMPLEMENTATION

We have implemented our model with ONOS Controller [8] and OpenFlow based access points as shown in Figure 2.
ONOS [8] adopts a distributed architecture for high availability and scale-out. The developers have used several modules such as switch manager, module management, link discovery and REST APIs from the Floodlight Controller. The data model in ONOS is implemented using Titan graph database, Cassandra key value store and the Blueprints graph API to expose network state to applications. The implementation of ONOS can be distributed across multiple servers and number of instances can be varied in accordance with the load. In distributed implementation, each server has a global view of the network but is responsible for managing subset of switches in the network. Hence any of the applications implemented on any instance of the Controller has access to the global view of the network. Applications read the global network view to make forwarding and policy deci-

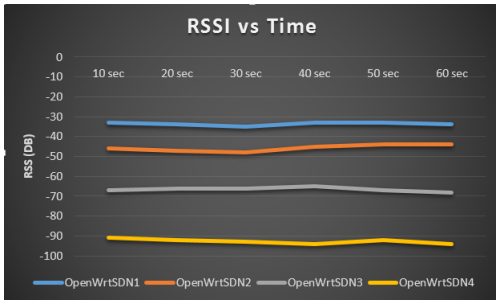

Figure 4: RSS vs Time

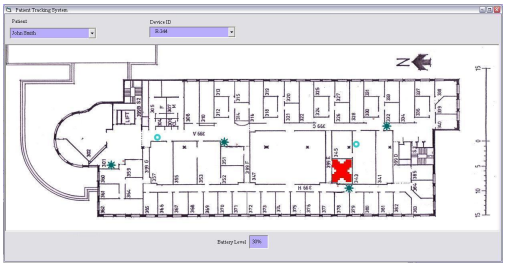

Figure 5: Patient Location

sions 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 [2]. 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.

Our prototype implementation makes use of a single ONOS Controller. As shown in Figure 3, we have developed monitoring application for ONOS for securing monitoring of the dementia patients. The security application have several sub-components for different purposes such as authentication, attacks detection, location detection and database components.

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 connected Controller. We have used a 6000mAH 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 4 shows a trace of RSS from different SDN AP in a particular time and from a particular tracking device.

We have implemented and tested our model in one of the university building on the third floor with sample hospital setup in some of the rooms. We have developed Arduino based wearable devices and also used Samsung mobile devices for tracking the patients. The green stars on the layout show the location of the OF-APs (OpenWrtSDNX). The OF-AP with the highest RSS is used as default OF-AP for providing access to the wireless devices and mobility of the users is detected by analysing the variations in the RSS. Also, the wearable devices are programmed to connect through specific OF-APs in their default location. In case where an OF-AP is not available or RSS falls below the threshold, the monitoring application assigns alternate OF-AP that can be used by the device. The RSS default value of -85 dBm threshold is used for changing the OF-APs for the wireless devices. The wireless devices are connected to the neighboring OF-APs if the signal strength is atleast 20 percent greater than the signal strength of the current OF-AP. Hence any operation from the wireless client devices that violate the configuration information raise an alert to the network administrator. 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.

The RSS and location information are stored in XML database and this information is used to train our model. We have captured a minimum of 15 training samples for each room. Also, since the patients will be spending most of the time on their beds, a minimum of 5 training samples were taken at different locations on the bed such as corners of the bed, centre of the bed and remaining samples from different locations such as toilet, fridge and room entry. Then we have tested our model with minimum of 10 samples by placing the wearable device at different locations in the room. We have achieved accuracy of 2 feet for the cases where the patient location is on the bed and accuracy of 1 meter for different locations in the floor layout.

Figure 5 shows the interface that can be used by the hospital staff to track the location of specific patient. The stars represent the location of OF-APs and blue circles on the map represent the sniffers which promiscuously capture the traffic on the wireless medium and monitor for specific events such as traffic matching with attack signature, unauthorized SSID broadcasts from rouge access points and events such as congestion. Query can be issued on the patient name or using the device ID. The results show the current location of the patient and the battery levels in the wearable device of the patient. Our current model raises alarms for the following specific events: i) high alert to nursing staff when patient location found to be leaving the default location (allocated room), ii) high alerts with the current location of the patients to the nursing staff when the dementia patients enter into the rooms of other patients iii) high alert to the

security staff when the patient is moving towards exit gate of the hospital, iv) medium alert to nursing staff when the battery level on the wearable device is at 20 percent and high alert when the battery level is 10 percent v) medium level alert to the network administrator during congestion and high alerts if traffic matching with attack signatures, vi) medium alert with the last known location of the patient to nurses when signals from wearable devices are not received for three successive intervals and vii) a high level alert with the last known location of the patient for nurses and security administrator if signals are not received for 5 successive intervals.

6. CONCLUSION

In this paper we have proposed techniques for making use of the SDN, WLAN and wearable devices of the patients for secure monitoring of the dementia patients in hospital environments. We discussed how SDN can help to resolve some of the challenges for real time monitoring of the patients and offers advantages for such critical applications. We have also presented a prototype implementation of our model using ONOS SDN Controller and OpenFlow access points.

7. REFERENCES

[1] http://www.alz.org/what-is-dementia.asp.

[2] Openwrt. https://openwrt.org/.

[3] A. Agiwal, P. Khandpur, and H. Saran. Locator: location estimation system for wireless lans. In *Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, pages 102–109. ACM, 2004.

[4] D. L. Algase, E. R. Beattie, and B. Therrien. Impact of cognitive impairment on wandering behavior. *Western Journal of Nursing Research*, 23(3):283–295, 2001.

[5] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill. Enhancing the security of corporate wi-fi networks using dair. In *Proceedings of the 4th international conference on Mobile systems, applications and services*, pages 1–14. ACM, 2006.

[6] P. Bahl and V. N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 775–784. Ieee, 2000.

[7] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *USENIX security*, pages 15–28, 2003.

[8] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, et al. Onos: towards an open, distributed sdn os. In *Proceedings of the third workshop on Hot topics in software defined networking*, pages 1–6. ACM, 2014.

[9] P. Dawson and D. W. Reid. Behavioral dimensions of patients at risk of wandering. *The Gerontologist*, 27(1):104–107, 1987.

[10] P. Enge and P. Misra. Special issue on global positioning system. *Proceedings of the IEEE*, 87(1):3–15, 1999.

[11] O. N. Foundation. Software-defined networking: The new norm for networks. https://www.opennetworking.org/images/stories/downloads/sdnresources/white-papers/wp-sdn-newnorm.pdf[Accessed12Dec.2015].

[12] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu. A timing-based scheme for rogue ap detection. *IEEE Transactions on parallel and distributed Systems*, 22(11):1912–1925, 2011.

[13] C. He and J. C. Mitchell. Security analysis and improvements for ieee 802.11 i. In *The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University, Stanford*, pages 90–110. Citeseer, 2005.

[14] B. Jordan. Emergency services find lost dementia suffere. http://www.greatfete.com.au/media/NewsLocal-HillsShireTimes-13Aug2013-Page3.pdf, 2013.

[15] S. Khan, K.-K. Loo, T. Naeem, and M. A. Khan. Denial of service attacks and challenges in broadband wireless networks. *8; 7*, 2008.

[16] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne. Vulnerabilities of wireless security protocols (wep and wpa2). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(2):34–38, 2012.

[17] C. K. Lai and D. G. Arthur. Wandering behaviour in people with dementia. *Journal of advanced nursing*, 44(2):173–182, 2003.

[18] H. Li, P. Li, S. Guo, and S. Yu. Byzantine-resilient secure software-defined networks with multiple controllers. In *2014 IEEE International Conference on Communications (ICC)*, pages 695–700. IEEE, 2014.

[19] C. Liu and J. Yu. A solution to wlan authentication and association dos attacks. *IAENG International Journal of Computer Science*, 34(1):31–36, 2007.

[20] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu. A security enforcement kernel for openflow networks. In *Proceedings of the first workshop on Hot topics in software defined networks*, pages 121–126. ACM, 2012.

[21] 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 Journal of Information Technology*, 6(4):441–446, 2007.

[22] A. Shalimov, D. Zuikov, D. Zimarina, V. Pashkov, and R. Smeliansky. Advanced study of sdn/openflow controllers. In *Proceedings of the 9th central & eastern european software engineering conference in russia*, page 1. ACM, 2013.

[23] S. Shin, Y. Song, T. Lee, S. Lee, J. Chung, P. Porras, V. Yegneswaran, J. Noh, and B. B. Kang. Rosemary: A robust, secure, and high-performance network operating system. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 78–89. ACM, 2014.

[24] P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Mitigating attacks on open functionality in sms-capable cellular networks. *IEEE/ACM Transactions on Networking*, 17(1):40–53, 2009.

[25] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, and X. Gao. A wireless lan-based indoor positioning technology. *IBM Journal of research and development*, 48(5.6):617–626, 2004.

[26] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 80–89. ACM, 2004.

[27] 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 *2009 International Conference on Advanced Information Networking and Applications*, pages 861–867. IEEE, 2009.