cellular network. Jin Chen et al. (2012) proposed a target network selection scheme based on bandwidth, dropping probability and cost parameters. Parameters are processed in target visiting network to reduce the processing delay. The rapidly changing network conditions make the collected metrics unstable. This requires frequent distribution of the collected metrics which increases the network traffic. Kirsal et al. (2013) proposed a Markov model for UMTS-WLAN integration based on predefined policies. This model clearly differentiates requests originating in the cellular network, from requests being handed over from WLAN to the cellular network. This ensures that calls handed over from WLAN to cellular network are not handed over back to the WLAN. This algorithm demands prediction of user movement, which makes it complicated to deploy it in a mobile terminal.

H. Liao et al. (2006) proposed fuzzy control theory based vertical handover decision algorithm which provides a generalized vertical handover decision procedure. In the proposed approach various input parameters are dynamically evaluated and computed to achieve optimized handover. L.Xia et al. (2007) proposed vertical handoff decision algorithm for overlay wireless networks consisting of cellular and wireless local area networks (WLANs). The proposed approach employs RSS prediction and pre-decision about target networks to achieve the expected QoS. Mehbodniya et al. (2012) proposed a fuzzy logic based multiple attribute decision making which includes received signal strength, QoS parameters, and mobile velocity attributes with analytic hierarchy process as a weighting scheme. Finally the target network is selected based on TOPSIS ranking algorithm. The above proposed algorithm considers most of the essential parameters for handover decision making. But, it does not consider the load on the target network. There is a chance that the target network may get overloaded with new incoming clients. In such cases, this algorithm will trigger unnecessary handover. Reddy et al. (2014) proposed an algorithm based on the dwell timer for eliminating ping pong effect by
reducing the shadow fading effect. But designing dwell timer for individual users based on their needs is not feasible.

Datta et al. (2012) proposed an analytic network process based optimum network selection algorithm using network traffic load, velocity of mobile station, reliability, data rate, and usage cost with the consideration of vehicular communication system. Lahby et al. (2012) and Kassar et al. (2008) proposed optimal network selection algorithm based on analytic network process and grey relational analysis. Maaloul et al. (2013) and Johnson et al. (2013) have presented a novel context aware vertical handover algorithm based on multiple attribute decision making and the results have shown that this algorithm avoids unnecessary triggered handovers. The imprecision of handover attributes in all these approaches may trigger unnecessary handover. Marquez et al. (2012) used geo-location, context information and route calculation for handover decision making to improve the performance of handover. But it requires high computational power to calculate geo-location based handover. There is no need to process entire available network list, because there may be a chance that some of the available network may have poor service quality (Ananthanarayanan 2014). In such cases, the processing of unsuitable network should be dropped at earlier stage itself. M.Gita et al. (2014) proposed a new approach of network priority based multi-criteria vertical handover decision algorithm. They claim that the proposed algorithm has improved network performance in terms of number of handoffs, network balance, and average blocking probability. E M Malathy et al. (2015) proposed a new approach by integrating TOPSIS method with dynamic programming approach to provide reduced handover failures as well as better QoS to end users.
2.3 TRAFFIC CLASSIFICATION

Even though internet traffic classification techniques are improving in accuracy and efficiency, the behavior of internet applications are changing rapidly. It makes the classification algorithm to exhibit high false positives. Routing particular application traffic without manual intervention requires clear identification of traffic origination. Bin Hu et al. (2012), Nguyen et al. (2008), and Dainotti et al. (2012) presented a survey about constructive analysis of the supervised and unsupervised traffic classification algorithms, achievements and obstacles to progress. Erman et al. (2006) presented an Expectation-Maximization algorithm based clustering algorithm for internet traffic classification and they have shown that their approach achieved an accuracy of 91%. If the number of clusters is large, then Expectation-Maximization algorithm creates outfitting problem. Yu Wang et al. (2010) proposed a method for Automatic Application Signature Construction from Unknown Traffic. Yu Wang et al. (2011) also proposed a classification algorithm using machine learning by pattern matching with common substrings in the payloads and reviewed the classification algorithms. Zander et al. (2005) proposed a novel method for machine learning based flow classification and application identification using statistical flow properties based on unsupervised machine learning. The average accuracy across all traces is 86.5%. But, these algorithms consider only a small set of data consisting of few thousands of samples and have shown that it takes minimum time (2070s for 8000 samples) and good accuracy (91.19%) to classify the dataset containing 8000 samples.
2.4 AUTHENTICATION PROCEDURE FOR UMTS-WLAN INTERWORKING

The target network may be utilizing a different radio access technology that increases the complexity in reducing the authentication delay. Existing protocols like EAP-TLS, EAP-Tunneled TLS use public key cryptography (Mishra A et al. 2004) that increases the signalling cost of handover, computation load and authentication delay. Pre-authentication (Ali Al Shidhani et al. 2009) of mobile station to the target network based on prediction of mobile station movement depends on the direction of the movement. If the prediction of movement fails, then the entire signalling will be unproductive. EAP-AKA protocol provides authentication services (SH Lin et al. 2010) using full authentication protocol with high authentication delay. In full authentication, the mobile station has to authenticate to HLR/HSS residing in the core network while moving away from 3G/UMTS to WLAN (Chou-Chen Yang et al. 2006) (Kwon H et al. 2006). This increases the computation in authentication server, reduces the performance of authentication server, and makes seamless handover impractical due to high authentication delay. 3GPP recommends the usage of fast re-authentication mechanism to reduce the authentication delay in order to support seamless mobility by handling the authentication in RADIUS server with acceptable packet loss (Arkko J and Haverinen 2006). But RADIUS server encounters high computation load due to the need for handling complete authentication procedure. Fast iterative localized authentication with minor changes to EAP-AKA protocol reduces the authentication delay by locally handling the authentication (Shen-Ho Lin et al. 2011). Performance studies made by Shen-Ho Lin et al. (2013) revealed that fast iterative re-authentication protocol improves the performance but, distributes the authentication vectors among multiple Access Points (AP) before verifying the legitimacy of the AP. This
flaw lets an intruder to capture the authentication vectors by running an illegitimate AP.

2.5 CO-OPERATIVE DECISION MAKING FOR LOAD BALANCING.

A number of proposals have been made for vertical handover decision algorithms. Ning Ding et al. (2013) presented collaborative Wi-Fi based offloading solution for energy conservation in smart phones. It collaborates cellular operators, Wi-Fi providers and smart phone users and offloads the mobile data to the nearest Access Point (AP) to conserve energy. However, this approach requires mobility prediction and localization algorithm for locating nearest AP, resulting in considerable expenditure of energy to be spent on localization process. The error in localization triggers unnecessary handover and network scannings. Kyunghan Lee et al. (2013) presented a quantitative study on the performance of offloading through Wi-Fi networks and it has been found that offloading saves 55% of battery power of smart phones. The theoretical framework estimates that the average performance of offloading in a given Wi-Fi deployment condition reduces the energy consumption. Dae Sun Kim et al. (2013) presented mobile velocity based offloading between 3GPP and non-3GPP access networks to reduce unnecessary network scanning. The variation in mobile velocity brings in uncertainty in decision making. Hence, along with mobile velocity, other factors like service cost, network latency, and user preferences etc., should be considered.

Picone M et al. (2013) presented an experimental analysis of mobile data offloading using Android application. Li Y et al. (2013) presented a mathematical framework to study offloading under realistic assumptions. The survey includes heterogeneity of mobile data, subscribing interest of
mobile users, and AP limitation in offloading. The authors used real mobility traces in simulation for testing Disruption Tolerant Networking. This model does not consider the network load on the target wireless network. Yongmin Choi et al. (2011) presented a quantitative survey and strategic solution for mobile data offloading and network planning.

Mehbodniya et al. (2012) proposed a fuzzy logic based multiple attribute decision making method, but it does not consider the load on the target network. There is a chance that the target network may get overloaded with new incoming clients. In such cases, this algorithm triggers unnecessary handover. 3GPP ANDSF and Hotspot 2.0 are the popular connection managers developed by 3GPP and Wi-Fi Alliance respectively for autonomous network discovery and connection. It is observed that these smart connection managers enable the mobile terminal to make decision based on network policy and received signal strength. But these popular connection managers do not consider the location information, access network type, and AP load while making a decision.

2.6 IMPROVED UTILIZATION OF PICOCELL USING CELL RANGE EXPANSION.

Underutilization problem of small cells should be addressed in the context of both base station and mobile station. At the base station, it can be implemented using multiple smart antennas to expand the region of small cells by controlling the transmission power of antennas. In the context of mobile station, expansion is possible by virtually expanding the region of small cell by adding expansion bias value to the received signal strength. Many Researchers concentrate only on mobile station side (Ismail Guvenc 2011) (Dhaval MT, Tanvi Shah 2014) (Kenta Okino 2011) (Koichiro Kitagawa 2012) (Andrews J G 2014) (Woo-Jong Jo et al. 2014). The
expansion bias value can be obtained either by centralized method or distributed method. In centralized method, expansion bias value is same for all UE. The expansion bias value is calculated and broadcast to all UE. In the distributed method, expansion bias value is different for different UE where each UE calculates its own expansion bias value.

Ismail Guvenc (2011) analyzed the benefits of range expansion with ICIC technique. Results show that whenever range expansion and ICIC is provided to HetNet, the overall user capacity is increased. Dhaval MT and Tanvi Shah (2014) proposed a cell selection scheme with priority queue where picocells get more priority. Whenever pico cells are available in the priority queue, the UE try to connect to the picocell having the maximum RSRP. This may lead to load unbalance between macrocells and picocells. Kenta Okino (2011) analyzed DL performance of UEs with various bias values under CRE with ICIC technique. Results proved that the moderate bias settings enhance the user throughput. Koichiro Kitagawa (2012) evaluated the performance of handover in CRE.

Fixed bias method is a traditional method where constant bias value is used for all mobile stations in the cell. The bias value may be calculated at base station and broadcasted to all mobile stations or preset to all mobile stations (Andrews J G 2014). Since each mobile station has different requirements, a common bias value will not be effective one. When bias value is high, user throughput will decrease since all mobile stations will try to connect to the same PBS even though they are getting very low RSS and there will be an added interference due to crowded devices.

Toshihito Kudo and Tomoaki Ohtsuki (2014) proposed a scheme to determine the bias value for each UE by using Q-learning algorithm, where each UE learns the bias value that minimizes the number of outage UE from
its past experience. Simulation results show that this scheme reduces the number of outage UE and improves network throughput. But, this method is difficult to implement in real time since it is learning from the number of outage UE, which is calculated at base station side and broadcasted to all mobile stations and number of the outages will vary according to number of UE present in the cell.

Shi-Sheng Sun et al. (2014) proposed a new scheme with rate-based CRE offsets in HetNet so that UE can decide on their associations based on their traffic demands. Each UE selects an appropriate cell according to the UE uplink traffic demand by using a rate-based CRE-offset mechanism. The UE with higher uplink traffic demands are assigned with a larger CRE offset. This model concentrates only on traffic demands, neglecting its battery level. It is important to protect the UE from power loss as well.

Woo-Jong Jo et al. (2014) proposed a model where cell range expansion depends on the number of random access resource available. The proposed model resulted in improved average random access efficiency and reduced average random access delay. PBS coverage is extended by controlling the transmission power of PBS. Transmission power varies depending on the difference between number of accessed UE and estimated number of UE. This approach is done in the base station side which requires modification in the architecture of MBS and PBS. Since base station approach is costly in many aspects, solution in mobile station side is needed.

### 2.7 RELIABLE AND SECURE COMMUNICATION IN WIRELESS PERSONAL MEDICAL DEVICES

Implementation of sensors in Wireless Personal Medical Devices (WPMD) results in wire-free communication between the medical devices on
the patients' body and provides mobility to the patients. In such health applications, more importance has to be given to data reliability and security of WPMDs. Wireless Sensor Networks (WSNs) that operate in the ISM band can be used in the medical devices for constant observation of patients’ health condition.

Food and Drug Administration (FDA), USA has approved the usage of Bluetooth - powered Blood Glucose Meter Insulin Pump Combo Systems for monitoring the blood glucose level. Since these devices involve communication of critical data, more focus is required on data accuracy and privacy.

Further, the guidance document drafted by FDA (FDA 2012) on design of RF wireless devices in medical devices and International Electrotechnical Commission's (IEC) document (IEC 2011) on necessary tests to reduce electromagnetic disturbances, also highlight the risks associated with the wireless data transmission in medical devices and the Electromagnetic Compatibility (EMC) of the wireless devices particularly in the ISM band. But the provisioning of system security has been mentioned as a feature and not as a requirement.

Due to rising interest in wireless sensors in WPMDs, a number of investigations on the reliable and secure wireless communication between WPMDs have been published recently.

The adversaries attacking the medical system can be classified into active and passive attackers. Active attackers have the capability to eavesdrop on traffic between the devices, network controller and the supervisor, inject messages, replay old messages, spoof, and ultimately compromise the integrity of device operation. Active attackers, if successful,
can not only invade a patient’s privacy but can also suppress legitimate data or insert false data into the network leading to unwanted actions or prevent legitimate actions. Faulty data received at the monitoring terminal may lead to wrong treatment and may leave the patient's life at high risk. Passive attackers, on the other hand, do not try to interfere with the operation of the medical devices.

In 2008, Professor Kevin Fu, a computer scientist at the University of Massachusetts Amherst, found that by capturing a signal, hackers can gain control of an implanted heart defibrillator with a wireless outlet. Fu found that implanted defibrillators are tested using a specific radio signal when been fitted inside a patient, and because the signal turns the device on and off, capturing and rebroadcasting the signal would switch the device off (Barnaby J Feder 2008).

In August 2011, Jerome Radcliffe stood onstage at the Black Hat Technical Security Conference in Las Vegas, hacked into the popular Medtronics wireless insulin pump that was affixed to his abdomen by a thin tube, and completely disabled it (Tiffany Kaiser 2011) (Jordan Robertson 2012) (Jim Finkle 2011). According to Radcliffe, an attacker could intercept wireless signals and then broadcast a stronger signal to change the blood-sugar level readout on an insulin pump so that the person wearing the pump would adjust their insulin dosage. If done repeatedly, it could kill a person (Darlene Storm 2011).

Radcliffe suggested scenarios where an attacker could be within a couple of hundred feet of a victim, like being on the same venue or on the same hospital floor, and then launch a wireless attack against the medical device. He added that with a powerful antenna, the malicious party could launch an attack from up to a half mile away. The only thing needed to launch
an attack is the serial number of the device. The serial number for his model was only six digits long, and Radcliffe wrote a computer program that was able to scan all potential combinations until it found the right one.

Another hacker, Barnaby Jack, who works for antivirus vendor McAfee, had also demonstrated problems with some of Wireless Personal Medical Devices, taking Radcliffe’s findings a step further by showing how to use an antenna to scan public places and attack pumps from up to 300 feet away without knowing the serial number of the device (Dan Goodin 2011).

Hence, there arises an increasing concern on the security and privacy aspects of the WPMD related to medical data such as data collection, data transfer and processing and maintaining electronic medical health records. By and large, security is not added to wireless medical devices, due to its limited battery life and memory, thus giving way to such vulnerabilities. The lack of security not only affects patients' privacy but it may also cause harm to the patient by allowing adversaries to interject spurious data ensuing in erroneous treatments. Furthermore, too much of security also causes problem to patient during emergency situations. Without the key, access will not be granted to the implanted devices putting the patient’s life at stake. So, there is always a trade-off between security and safety of the WPMD.

2.8 CONCLUSION

This chapter presents the published literature in the area of vertical handover techniques in wireless heterogeneous networks to provide seamless and secure handover. A detailed literature survey about security challenges related with wireless personal medical devices is also discussed. A number of issues such as handover delay, authentication, reliable and secure communication of data in HetNet and WPMDs are presented in this work.
From the literature survey, it is observed that the current algorithms and systems work under various limitations and difficulties in practical implementations. Based on the studies done, it is clear that there is still a demand for evolving more robust and secure vertical handover algorithms to meet the demands of end users as well as service providers. Various algorithms and systems are proposed in this research work to provide solutions for a subset of issues addressed.