Int. J. Communications, Network and System Sciences, 2014, 7, 131-140
Published Online May 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.75015

Scientific Research

Application of Machine-Learning Based Prediction Techniques in Wireless Networks

Gitanjali Bhutani

WCDMA, Alcatel-Lucent Technologies India Private Limited, Bangalore, India
Email: gitanjali.bhutani@alcatel-lucent.com

Received 18 April 2014; revised 30 April 2014; accepted 7 May 2014

Abstract

Wireless networks are key enablers of ubiquitous communication. With the evolution of networking technologies and the need for these to inter-operate and dynamically adapt to user requirements, intelligent networks are the need of the hour. Use of machine learning techniques allows these networks to adapt to changing environments and enables them to make decisions while continuing to learn about their environment. In this paper, we survey the various problems of wireless networks that have been solved using machine-learning based prediction techniques and identify additional problems to which prediction can be applied. We also look at the gaps in the research done in this area till date.

Keywords

Wireless Networks, Prediction, Machine Learning, Ubiquitous Communication, Pervasive Computing

1. Introduction

In the current age of Information Technology revolution, quick availability of use of information to make speedy decisions is becoming a competitive advantage for many businesses. In such an environment, to have all decision-makers connected in, ubiquitous communications have become the need of the hour. Ubiquitous computing and communication combine mobility with context awareness, adaptability, scalability and localization to create an environment where devices are smarter and take actions by predicting user behavior. It finds its applications in a large variety of areas including energy conservation, manufacturing, healthcare, banking, education and telecommunications. In order to make ubiquitous computing a reality, certain devices are absolutely necessary. At the bottom of this ubiquitous computing stack, there are the sensors or smart phones with sensor functionality. These are responsible for collecting information from the surrounding environment and reporting it to a deci-

How to cite this paper: Bhutani, G. (2014) Application of Machine-Learning Based Prediction Techniques in Wireless Networks. *Int. J. Communications, Network and System Sciences*, **7**, 131-140. http://dx.doi.org/10.4236/ijcns.2014.75015

sion-making entity. In order to allow these sensors to communicate, the next layer is the wireless communication layer which can be provided by the 802.11 family of networks or any other communication technology. The final level in the stack includes the applications that collect, mine and analyze the data collected by the sensing devices for patterns in order to make decisions. Wireless networks, being a key enabler of the ubiquitous communication paradigm are gaining in importance. The quality of service provided by these networks is of utmost importance in determining the applications that they will be put to. Not only do these networks have to provide an enhanced quality of user experience (QoE), they must do so at optimized rates and with optimum resource usage. Wireless devices are extremely constrained for power and the network implementations have to account for this at all times.

With smart-phones being used for newer real-time applications every day, it becomes challenging for the wireless network elements to keep pace. It is thus the need of the hour for networking software to adapt to changing requirements and user trends without the need for manual intervention. One way of achieving this is to build intelligent network elements that record user behavior, characterize it, identify patterns in it and use the knowledge gained from these data to adapt various parameters. Foremost in the requirements of this type of intelligent software is the ability to predict different aspects of user behavior in order to determine any parameter changes or other actions sufficiently in advance, so that changing network conditions, due to mobility or other reasons, are seamless for the user. The use of artificial intelligence, specifically learning and prediction techniques make these adaptable systems a reality.

In this paper we look at the applications of prediction techniques to solve different aspects of the ubiquitous computing problem. The remaining part of the paper is organized as follows: in Section 2, we discuss machine learning techniques for prediction in more detail; Section 3 categorizes the literature in the area of prediction in wireless networks, based on the problems addressed using prediction; Section 4 and beyond look at each of these areas in further detail and compare the various methodologies used; finally, we look at the research gaps in this area of building intelligent wireless networks using prediction techniques.

2. Overview of Machine Learning

Machine learning deals with algorithms that give computers the ability to learn, in much the same way as humans. This means that given a set of data, an algorithm infers information about the properties of the data, allowing it to make predictions about other data it may see in the future. The main focus of machine learning is the design of algorithms that recognize patterns and make decisions based on input data. Machine learning has found uses in areas like biotechnology, fraud detection, wireless networks, stock market analysis and national security.

Machine learning algorithms can be categorized into:

1) Supervised learning: these set of algorithms use training data to generate a function that maps the inputs to desired outputs (also called labels). For example, in a classification problem, the system looks at example data and uses it to arrive at a function mapping input data into classes. Artificial neural networks, radial basis function networks and decision trees are forms of supervised learning.

2) Unsupervised learning: these set of algorithms work without previously labeled data. The main purpose of these algorithms is to find the common patterns in previously unseen data. Clustering is the most popular form of unsupervised learning. Hidden Markov models and self-organizing maps are other forms of Unsupervised Learning.

3) Semi-supervised learning: as the name indicates, these algorithms combine labeled and unlabeled data to generate an appropriate mapping function or classifier.

Artificial neural networks are extremely popular in the field of prediction in wireless networks. The other techniques like decision tress and unsupervised learning are used much lesser. Experiments prove that using a combination of techniques instead of a single one provides the best results.

3. Survey of Prediction Techniques in Wireless Networks

As wireless networks move towards being omnipresent to facilitate smart homes, offices and so on, completely eliminating any manual intervention in setting these up and operating them is essential. In order to adapt to the environment and inter-operate with other systems, making these systems intelligent will be essential for their success. One of the main problems in wireless networks is the unpredictable signal quality. The signal strength

at any point in a wireless network is impacted by several factors—topology of the area, presence of buildings, interference from different networks and appliances operating at similar frequencies and so on. Since, the networks or the neighboring devices can keep changing, having a static algorithm to attack this problem will not work. Instead, having wireless network elements sense interference and respond to it appropriately will allow adaptation to changing environments. One of the most researched areas in ad-hoc and wireless sensor networks is in wireless link status prediction. Being able to predict when a link's strength will drop below threshold levels and for how long, will allow applications to take corrective action in advance, thus ensuring minimal service disruption. Section 4 looks at the application of machine learning to this problem.

As the different types of networks and devices multiply, it is essential to allow inter-operability amongst these to give users maximum flexibility. Amongst other aspects, achieving inter-operability involves achieving seamless handovers between these networks. Different schemes exist to ensure a seamless handover between networks, but to complete the handover in time with minimal wastage of resources requires prediction of the time at which the mobile station will lose connectivity to its current network. This prediction of mobility and disconnection time is the focus of Section 5.

The most researched areas in ad-hoc and wireless sensor networks are those of routing and intrusion detection. The ad-hoc nature of these networks means that mobile nodes are responsible for routing packets while processing their own data, but users can enter and leave the network at any time. The main focus of research in this area is to have routing algorithms that can adapt to the changing topology as quickly as possible. Having some amount of prediction capabilities built into these algorithms allows them to select the most reliable and longer duration routes to forward data. Section 6 looks at the use of prediction in routing in further detail. The ad-hoc nature of these networks also makes them extremely vulnerable to security attacks. With the emergence of newer forms of security threats all the time, being able to use the data from previous attacks to predict the general characteristics of attacks and to detect newer ones will go a long way in securing these systems. Use of prediction in intrusion detection is the main focus of Section 7.

4. Wireless Link Status Prediction

The stability and reliability of links in wireless networks is dependent on a number of factors such as the topology of the area, inter-base station or inter-mobile station distances, weather conditions and so on. As such, there is no single way of modeling wireless link behavior that will work in all cases, making it difficult to predict wireless link availability using mathematical models. At the same time, an estimation of link quality and link availability duration can drastically increase the performance of these networks, allowing the network to take proactive measures to handle impending disconnections. One such application of link disconnection prediction is discussed in [1], wherein the authors propose a scheme that prevents Transmission Control Protocol (TCP) congestion control mechanism from kicking in during temporary disconnection of a Mobile Station (MS). Having been designed for wired, fixed networks, TCP interprets all delayed acknowledgements and packet losses as congestion and brings its congestion control mechanisms into operation. These mechanisms can lead to a huge reduction in data rates as seen by the MS and is wasteful if a MS experienced disconnection due to transient network conditions, which is rather normal in wireless networks. In the scheme proposed in [1], a base station measures the signal strength for each MS and uses it to predict the time and duration of disconnection. Based on the predicted time, it starts caching Transmission Control Protocol (TCP) Acknowledgements (ACKs) for the MS that is going to be disconnected. When the MS is disconnected, the stored ACKs packets are then spaced out in time for the duration of the disconnection, in order to prevent the TCP source from bringing its congestion control mechanisms into play, on detecting lost packets. Another application that would greatly benefit from the wireless link predictions is that of routing in ad-hoc and wireless sensor networks. While routing itself is a challenge in these networks due to node mobility and the absence of a fixed infrastructure, it becomes further complicated if the routing algorithm does not take the link lifetime into account. This can lead to numerous re-routings, degrading the performance of the network. These two applications are only a few of the plethora of applications that would benefit from the ability to predict the wireless link quality well in advance. In this section, we look at some of the research done in this area.

Another scheme for link quality prediction and link estimation called 4C [2] uses previously collected link quality data to construct three different machine-learning models: Naïve Bayes classifier (supervised learning technique that is built using the Bayes theorem and is used to classify previously unseen data based on the

learning that was performed in the training stage), logistic regression (a statistical technique that predicts the probability of the dependent variable having a particular value based on the values of the independent variables) and artificial neural networks. These models are constructed based on a combination of Packet Reception Rate (PRR) for link estimation and Received Signal Strength Indicator (RSSI), Link Quality Input (LQI) and Signal to Noise Ratio (SNR). The output of each model is the success probability of delivering each packet. Once the models are trained, they are deployed for prediction, with the error from each prediction being fed back to the models to continue the learning process. The authors compare the prediction accuracy of each of these models against a Bernoulli process whose success probability is set to the packet reception rate. Experimental results show that all three models have a greater prediction accuracy than the Bernoulli process with the Logistic regression model having the best accuracy at very low computational cost. The authors also compare the 4C algorithm against other similar estimator algorithms like 4 Bit [3] and Short Term Link Estimator (STLE) [4] and find a 20% to 30% difference in accuracy with 4C performing the best.

In order to predict wireless network connectivity, that is, the signal to noise ratio for a mobile station, [5] proposes the use of a new Taylor Kriging model, which is basically the Kriging model with third order Taylor expansion for prediction. The Kriging technique is an interpolation technique used to estimate the value of a mathematical function at unknown points, based on the values at known points. It tries to fit the function to a specified number of points. The authors compare the accuracy of the Taylor Kriging model against that of a predictor built using the Ordinary Kriging model [6] and an artificial neural network based predictor [7]. The authors use wireless data sets which contain the power of a tower at particular points and the Euclidean distance of these points from the tower. This is used as input to the models built in [5]-[7]. For each point, the output of the model is the logarithm (to the base 10) of the signal to ratio value for that point. The prediction accuracy of the Taylor Kriging model is significantly higher than that of the models proposed in [6] and [7], especially when it comes to constrained training sets. However, the experiments prove that in absolute terms the prediction error is still substantially high.

5. Handovers and Prediction

In this section, we look at prediction to facilitate smooth handovers in further detail. Given the ubiquitous computing environment, together with the smart devices that can support multiple technologies and the application requirements to stay connected all the time, handovers across technologies are more widely supported and researched than in the previous generation of technologies. Handovers can be classified into:

1) Horizontal Handovers: these are handovers between same technology base stations.

2) Vertical Handovers: these are handovers between base stations belonging to different technologies, and as such are more challenging to handle than horizontal handovers. This is because of the variable handover times depending on the target network, together with the different procedures involved in handover.

Prediction to facilitate smooth handovers involves being able to predict the next location or point of attachment of mobile stations. Being able to predict the next location well in advance allows evaluation of candidate target networks to determine which one best meets the requirements, reservation of resources in the target network to avoid ping-pong of handovers and minimal loss of data since, the handover can be completed just as the mobile station loses connectivity to its current network. Prediction of the next location of a mobile station is also called mobility management. A lot of the literature in this area like [8] [9] look at a user's past movement history and predicts future movements and locations. These mechanisms primarily differ in the information used to predict the user's location. Some schemes like [8] look at only the current location of the user and the historical movement information to predict the future location. In this paper, the authors use a Hidden Markov Model to predict the user's next location. They use real trace datasets to train the model. The model continues to be tuned as it is used for prediction in the network. A Markov chain model is used in [9], in order to predict the user's next location. The disadvantage of the Markov chain model is that it only takes the user's previous location into account. Such a model misses the different paths that different users can take to reach the same state, thus severely affecting the accuracy of the model. In contrast [8] uses a k-th order Markov model, where $k > 1$. In this case, the system records the movements of the users for the past k transitions. The Access Point (AP) controller is responsible for collecting data from APs about transitions and using this data to predict the next location of the user. The AP controller constructs an HMM for each user and uses this to make predictions. Using an available campus wireless dataset [10], the authors build the HMM and use it to make predictions and measure the

prediction accuracy of the model. The data mined from the datasets provides interesting insights into user movements, the notable one being that most users connect to one or two APs most frequently. The prediction accuracy of the model is impacted by this nature of the dataset and hence, it is easily able to predict if a user will connect to one of its favored APs rather than one of the APs that the user rarely visits. In addition, the experiments also prove that the prediction accuracy falls with the increase in sequence length.

Other schemes use information like network topology and delve deeper into user characteristics to be able to predict the user's next location. One such technique is described in [11], where users are classified into groups, with all users of a group having similar movement patterns. The paper discusses a technique called Behavior Based Mobility Prediction (BMP), which uses the user group, location, time-of-day and duration in a cell information to predict a user's next point of attachment. The location represents the history of mobility patterns—the movement history of all mobile stations is recorded. The location information together with information about the direction in which the mobile station is moving allows the user's next location to be predicted. This method allows the structure of buildings and layouts of roads to be taken into account in the next location prediction. The time-of-day factor represents the fact that user movements differ based on the time of the day. The duration factor captures the user's speed of movement through a cell and is categorized as short, medium and long. The authors specifically look at the problem of handoff latency in wireless LANs. The main reason for the large handoff latency in Wireless LANs is the time needed for scanning for new Access Points (APs) when moving from one cell to another. The authors argue that predicting the next point of attachment of a Mobile Station (MS) can eliminate the scanning overhead and correspondingly reduce the handoff delay. Short duration reflects an unnecessary handoff. Such handoffs can be eliminated by next location prediction using BMP.

The BMP scheme is assumed to be implemented by a server which can be co-located with the authentication server. The server uses all of the user's movement and location characteristics, together with the time of the day, to arrive at prediction lists consisting of next points of attachment for the MS. The MS then re-associates with the AP in the cells specified in the prediction list in order of their appearance in the list, if associations fail. During the next handoff, the first prediction in either list is used as the next cell prediction based on whether the duration of the MS in the current cell is medium or long. If the first prediction fails, the second is used and so on. A full scan is performed when all the predictions in the lists fail.

The authors compare the BMP technique to other techniques that are used to predict a user's next location, such as determining next location based on signal strength, employing extra devices or an overlay network to detect APs and so on. BMP scores over these techniques because none of them can completely eliminate the need for scanning for APs, nor do they take the location topology or structure into account. The authors argue that the other prediction schemes that exist in the literature do not take the nuances of WLANs into account such as highly overlapped cells and MAC contention. In addition, the location-based schemes cannot capture mobility patterns that deviate from the norm.

Another category of literature that tries to solve the vertical handoff problem (handoff across technologies) is based on the IEEE 802.21 standard that defines a middle ware architecture to ease handoff across technologies, called Media Independent Handover Functions (MIHF). The architecture defines the Event Service which provides information about change in local and remote link layer conditions in the form of events and triggers. These triggers include: 1) Link Up (LU), 2) Link Down (LD), 3) Link Going Down (LGD), 4) Link Going Up (LGU). The LGD trigger leads to the network triggering a handover for the corresponding mobile station. Receiving this trigger too late means that the link will be lost before the handover is complete and hence, there will be data loss. Receiving this trigger too early means that there will be a wastage of network resources, since the link was still working in the source network when the handover occurred. Hence, the right timing of these triggers is essential for an efficient handover. Thus, a large body of literature in this area attempts to find different mechanisms to predict the timing of these triggers. We discuss some of it in this section.

The algorithm presented in [12] uses linear prediction to predict the signal strength at the source and target networks in order to obtain the handover initiation time. The authors define the threshold signal level at which the prediction of signal strength must start to be a certain factor greater than the signal strength at which the signal is lost.

As the signal strength approaches this level, the prediction of the source network signal strength starts. The prediction process ends when the signal is lost. At this point, the MS should be able to connect to the target network for a seamless HO. Hence, the time taken to initiate and execute the HO is taken into account to calculate the time at which the prediction of the target network signal strength starts. This prediction continues until

the predicted signal strength crosses the level at which the MS can safely connect to the target network without losing any data. The authors compare this scheme to the scheme used in [13], which predicts the signal strength of current and target base stations, but the HO trigger time is the average of the link up and link down time. The link up time is when the predicted Received Signal Strength (RSS) at the current base station goes below the threshold and correspondingly, link down time is when the predicted RSS at the target base station goes above the threshold. The authors argue that this scheme leads to an increase in the probability of unnecessary HOs in overlapping networks, which is overcome with the scheme they propose. Other schemes like [14] use only prediction of the RSS of the current BS to obtain the LGD indication. But this may lead to a HO being triggered when there are insufficient resources in the target network, which is overcome by the prediction of the RSS of both source and target networks.

A cross-layer predictive handover architecture based on the 802.21 standard is proposed in [15]. This work differs from any of the others, in that the LGD is not triggered based on just RSS predictions, but it also takes into account the time taken to perform a handover to the identified target network. The link down trigger from layer-2 typically results in a multitude of actions at layer-3 to complete the handover, and the time required for these is different based on the target network type chosen. Hence, not taking the target network type into account can lead to very early or very late handover initiations. The authors propose a handover control layer between layer-2 and layer-3 which stores the MIHF related information, thresholds and the handover decision engine. When the RSS of the MS goes below the InitAction threshold configured at this layer, the MS starts a process of neighbor network discovery and evaluation. This is done with the help of the Information Services of MIHF. Using this information, the handover time is then determined. The MS then tries to predict the time at which the signal will go below the threshold and using this and the handover time, triggers the LGD event at an appropriate time. Using simulations, the authors prove that the proposed mechanism leads to minimal service disruption times and almost zero early triggering costs. A similar mechanism of using neighboring network information to determine the time for LGD is proposed in [16].

6. Prediction in Routing and Position Estimation

Ad-hoc networks and wireless sensor networks are growing in popularity because of the limited infrastructure needed to make these networks a reality and the self-organizing nature of these networks. The self-organizing nature of these networks is an area of active research due to the need for the networks to mimic the operator's intelligence in configuring and maintaining themselves. One such prominent research area is that of packet routing in these networks. Since, these networks work based on different mobile stations serving as intermediate hops, changes in topology and thus routing paths are very frequent. Routing algorithms that adapt to these changing topologies while consuming minimal energy are an important requirement in these networks. This section looks at how prediction techniques can be used to overcome some of the routing problems in ad-hoc and sensor networks.

In [17], the authors propose a secure and reliable routing framework for Wireless Body Area Networks (WBANs). Wireless body area networks consist of a network of sensors to monitor bodily functions. The data from these sensors is then aggregated and sent over the Internet to a central monitoring entity. Although these networks are small in size and extremely localized, bodily movements subject them to frequently changing topologies and correspondingly the routing algorithms must adjust to this quickly to allow reliable data transfer of critical data. The authors propose a framework in which each node measures the link quality of all its neighbors. Using past link quality measurements, the nodes predict the incidental quality of a link using an auto-regression model. Auto-regression models are used for modeling of time-series data and to predict the value at a particular instant of time. When the routing algorithm has to select among a set of candidate nodes, it uses the one with the best link quality. When a node sends a data packet, each node listens to the transmission even though it is not destined to it. These nodes respond back with an ACK to the sender node, the ACK packet containing the received signal strength. The sender node uses this to update the link-quality measurement that it maintains. A node which does not respond with an ACK is marked as unreachable by the sender node. Through simulations, the authors prove that the proposed technique improves the routing reliability because one of the best links is chosen for transmission at each point, and the probability of sending a packet to a dead or a non-existent node is minimal.

Cognitive radio is a technology devised to overcome the spectrum shortage problem, by allowing unlicensed

users (also called Cognitive Users—CU) to use the unused parts of the spectrum originally allotted to Primary Users (PU). Towards this end, individual nodes sense their environment and adjust their transmission parameters to minimize interference with primary users. While this allows extremely efficient spectrum utilization, it makes routing a challenge in these networks, where the chances of interference with primary users are much higher and thus the links are unreliable and available for shorter durations. The application of prediction-based algorithms to the problem of topology control and reliable routing in cognitive radio networks is discussed in [18]. The authors argue that the routing algorithms must take the link availability into account when choosing next hops. This paper proposes a distributed prediction-based cognitive topology control scheme to provide this capability to the routing layer. In order to provide a minimal risk solution, this scheme is built into a separate layer between the cognitive radio layer and the routing layer to avoid making changes to well-established routing algorithms like AODV, DSR and distance-vector routing. This layer is referred to as the cognitive topology control layer and works to establish a reliable topology for routing protocols to operate on. This topology is constructed by using a new link reliability metric, determined based on:

1) Link availability time, predicted using the scheme proposed in [19],
2) Period of time spent in re-routing,
3) Link data rate.

This reliability metric is used to determine the weight of a link and the weight of a path. The algorithm then proceeds to construct the topology, by identifying all neighbors, estimating the path weights from initial node to unvisited nodes and then constructing the complete topology using the paths with maximum weight. This ensures that re-routings are minimized because using the path weight equation, links with high data rate and low availability time and links with low data rate and high availability time are avoided as far as possible. This allows the routing algorithms to indirectly take into account the mobility of CUs as well as the interference from PUs in routing decisions. Through simulations, the authors prove that the resulting routes are more reliable and lead to lesser re-routings.

The algorithm proposed in [20] performs routing based on link lifetime and coverage area. In this case, the energy drain rate is used to predict the link energy and the movement is calculated by relative motion estimation. Using this information, the packet can be routed on a path with a longer lifetime and lesser chances of packet loss.

7. Prediction and Intrusion Detection

The emergence of ad-hoc and wireless sensor networks has brought in several advantages like efficient utilization of the spectrum, reduction in Capital Expenditure (CAPEX) due to the absence of a fixed infrastructure, reduction in Operating Expenditure (OPEX) because of their self-configuring nature and allowing much better monitoring of military areas and making wireless body area networks and ad-hoc vehicular communication a reality. However, greater flexibility also makes these networks more vulnerable to security threats and attacks. Hence, different authentication mechanisms, attack detection and attack prevention mechanisms have been studied extensively. However, increase in the computing power allows large equations and passwords to be broken in a matter of seconds and hence, security algorithms need to keep evolving to keep finding and fixing newer and newer vulnerabilities. In all cases of network security, detection of an attack or a security threat is the biggest challenge. In this section we look at the use of machine learning techniques to detect intrusion and denial-of-service attacks in ad-hoc and wireless sensor networks.

The algorithm presented in [21] uses support vector machines to detect a Denial-of-Service (DoS) attack in mobile ad-hoc networks. Support Vector Machine (SVM) is a machine-learning technique used for regression as well as classification. In this case, the authors use the SVM as a classifier, to classify packets as normal or attack. The packets classified as attack packets are dropped by the network. Two datasets-one of normal traffic and one of an abnormal attack are used to train the SVM classifier. Since, attacks are continuously evolving, their detection requires the algorithm to learn like the human brain does as detailed in [22]. The authors propose a three-layer hierarchical brain-like learning algorithm for intrusion detection and prediction in wireless sensor networks. The authors contend that intrusion detection schemes cannot contain the damage that intrusions cause, because by the time they detect the intrusion, it has mostly passed. So they propose a technique that predicts and detects intrusion. The scheme uses three layers and four agents to detect and predict intrusion:

1) The supervised learning layer resides in the individual sensors. A decision tree is used as a classifier to

perform this supervised learning. The decision tree is contained within the detection agent. This agent uses a set of rules to drive the classification process of the tree. The results of the classification are further used to update the rules. If an attack that is unknown to the sensors occurs, it is sent to the sink node.

2) Unsupervised learning performed at the sink. A decision tree is used to perform clustering at the base station. If an attack unknown to the sink occurs, it is propagated to the base station.

3) Reinforcement learning performed at the base station: reinforcement learning is used to predict intrusion in advance. The authors use a convergent temporal-difference learning scheme [23] in this layer to predict an intrusion. Whenever an attack is detected by the sensor or sink, it is reported to the base station which uses this to further build its prediction system. The prediction system consists of the input layer, the output layer, the hidden layer and the stochastic layer. Temporal-difference learning is used to update the weights. The prediction agent contains the logic to implement intrusion prediction based on reinforcement learning.

The database agent logs all events and attacks and provides an interface for querying by the detection and prediction agents. The communication agent facilitates communication between the sensors, sinks and the base station.

The authors evaluate the time overhead, memory consumption and communication overhead of this scheme in addition to its prediction accuracy. The algorithm is found to have the lowest time overhead as compared to the schemes proposed in [24] [25]. The energy consumption in detecting an attack is obviously greater than the energy consumption in a normal operating sensor, but is only marginally greater for an unknown attack versus a known attack. The prediction rate is found to be 12 percentages higher than that of the SGA based scheme proposed in [26].

A scheme to detect malicious nodes based on energy prediction is proposed in [27]. Most schemes use node interactions or traffic profiles to detect an intrusion. However, this scheme uses the energy consumption of a node to detect an attack in cluster-based wireless sensor networks. The sensors consume energy in one of 4 states: 1) transmitting, 2) receiving, 3) sensing, 4) calculating. The authors propose a means for predicting the energy consumed by a sensor by having the cluster head calculate the probability that each sensor node will move from one state to the other in a given set of time slots. Using this probability, the energy dissipation for those set of time slots is predicted. At the start of each time period, the cluster head predicts the energy dissipation of each sensor. At the end of each time period it determines the remaining energy levels at each sensor. If the actual energy consumed deviates largely from the predicted dissipation, it is classified as an attack and the node is blacklisted. A blacklisted node is removed from all routing tables and is thus isolated from the network. The authors also provide a means for determining the type of attack the malicious node is involved in by characterizing the energy dissipation deviation for five different types of attacks, namely:

1) Selective forwarding attack: in this case, the energy dissipation is lower than the predicted value.

2) Hello flood attack: substantially higher energy dissipation than predicted.

3) Sybil attack: difference in energy consumption is larger than a preset threshold.

4) Wormhole attack: double the predicted energy is consumed.

5) Sinkhole attack: difference in energy dissipation increases gradually.

Simulation results show that the scheme is more efficient than existing ones in that it has high prediction accuracy and does not require any monitoring at individual sensor nodes. As a result, it can detect attacks with the least energy consumption which is ideal for limited-resource networks like wireless sensor networks.

8. Research Gaps

A large portion of the research in wireless networks relies on knowing the status of the link as reliably as possible. The wireless link prediction schemes predict the time at which the signal quality will degrade. However, these are looked at mostly from a handover perspective. Several times, the signal quality degradation is a transient condition because of environmental factors and do not eventually lead to a handover. As such, using historical data to predict disconnection duration would be instrumental in a lot of applications like video streaming, browsing sessions based on TCP and so on. Being able to predict the disconnection duration in non-handover scenarios is thus a gap which needs to be researched in more detail.

Most of the research in the area of imparting intelligence to network elements uses artificial neural networks to perform prediction. With machine learning itself being an active area of research, a lot of newer models have been formulated and several experiments run to prove that these work better than artificial neural networks.

Techniques like Random Forests and Deep Learning have been proven to achieve high prediction accuracies. Applying these techniques to the current wireless network problems and comparing their accuracy against that of artificial neural networks will help to establish the feasibility of these techniques and set the stage for their usage in wireless network research.

The other area that needs to be looked at in further detail is the efficient implementations and resource consumption of machine learning techniques in real-time devices. While there is a large body of literature that uses machine learning techniques to solve problems in wireless networks, only a small portion of it actually looks at how efficient and resource-usage friendly each of the techniques is. Given the computation intensive nature of some of the algorithms, it is perfectly possible that they lead to extremely accurate predictions but cannot be employed in any of the devices because of the resource consumption involved. Evaluating the various techniques based on their resource consumption in different systems is thus a topic that needs further work. In addition, research in the area of building efficient implementations of machine learning techniques for wireless networks, which take into account the limited memory, computing power and battery life in these networks is imperative.

Finally, all machine learning models are heavily dependent on the availability of real datasets. Today, there are few datasets available [10] and these are used by researchers to validate their experiments. The usability and ease of deployment of machine learning prediction techniques will be determined by how well the models have been trained and tuned. Having unrealistic models can lead to side-effects on the network causing service disruption and wastage of resources. Concentrated research effort thus needs to be spent on determining how realistic datasets can be generated or how these can be captured from the network without side-effects to the user and the network operator.

9. Conclusion

An ever-increasing customer base and the need for ubiquitous computing pose new challenges to network operators. The network elements must be able to continuously evolve with the user demands. This is only possible if they are designed to adapt to changing network conditions. Building adaptability into a system involves providing it with some level of intelligence that enables it to take decisions in different situations. In this paper, we looked at the application of prediction techniques to different wireless network problems like handover latency reduction, routing, link duration prediction and so on. In most cases, these techniques provided a significant improvement over their static counterparts. The large body of research in this area also indicates that the industry is slowly but surely realizing that systems have to be more and more adaptable in order to be able to handle the data explosion. As more machine learning techniques evolve, researchers are beginning to look at more un-orthodox techniques that give higher prediction accuracy and are less performance-intensive. A considerable amount of effort is also being put into adapting existing techniques for use in real-time systems.

References

[1] Bhutani, G. (2010) A Near-Optimal Scheme for TCP ACK Pacing to Maintain Throughput in Wireless Networks. *Proceedings of the* 2*nd International Conference on Communication Systems and Networks*, Bangalore, January 2010, 491-497.

[2] Liu, T. and Cerpa, A.E. (2011) Foresee (4C): Wireless Link Prediction Using Link Features. 2011 10*th International Conference on Information Processing in Sensor Networks* (*IPSN*), Chicago, 12-14 April 2011, 294-305.

[3] Fonseca, R., Gnawali, O., Jamieson, K. and Levis, P. (2007) Four-Bit Wireless Link Estimation. *Proceedings of the Sixth Workshop on Hot Topics in Networks* (*HotNets VI*), Atlanta, 14-15 November, 2007.

[4] Alizai, M.H., Landsiedel, O., Link, J.Á.B., Götz, S. and Wehrle, K. (2009) Bursty Traffic over Bursty Links. *Proceedings of the* 7*th ACM Conference on Embedded Networked Sensor Systems*, New York, 4-6 November 2009, 71-84.

[5] Liu, H., Al-Khafaji, S.K. and Smith, A.E. (2011) Prediction of Wireless Network Connectivity Using a Taylor Kriging Approach. *International Journal of Advanced Intelligence Paradigms*, **3**, 112-121. http://dx.doi.org/10.1504/IJAIP.2011.039744

[6] Konak, A. (2009) A Kriging Approach to Predicting Coverage in Wireless Networks. *International Journal of Mobile Network Design and Innovation*, **3**, 65-71. http://dx.doi.org/10.1504/IJMNDI.2009.030838

[7] Capka, J. and Boutaba, R. (2004) Mobility Prediction in Wireless Networks Using Neural Networks. *Management of Multimedia Networks and Services*, **3271**, 320-333. http://dx.doi.org/10.1007/978-3-540-30189-9_26

[8] Prasad, P.S. and Agrawal, P. (2010) Movement Prediction in Wireless Networks Using Mobility Traces. 7*th IEEE Consumer Communications and Networking Conference* (*CCNC*), Las Vegas, 9-10 January 2010, 1-5.

[9] Prasad, P.S. and Agrawal, P. (2009) Mobility Prediction for Wireless Network Resource Management. 41*st Southeastern Symposium on System Theory*, Tullahoma, 15-17 March 2009, 98-102.

[10] Crawdad: Wireless Traces from Dartmouth. http://crawdad.cs.dartmouth.edu/

[11] Wanalertlak, W., Lee, B., Yu, C., Kim, M., Park, S.M. and Kim, W.T. (2011) Behavior-Based Mobility Prediction for Seamless Handoff in Mobile Wireless Networks. *Wireless Networks*, **17**, 645-658. http://dx.doi.org/10.1007/s11276-010-0303-x

[12] Pahal, S., Singh, B. and Arora, A. (2013) A Prediction Based Handover Trigger in Overlapped Heterogeneous Wireless Networks. 2013 *IEEE International Conference on Signal Processing, Computing and Control* (*ISPCC*), Solan, 26-28 September 2013, 1-6.

[13] Yan, J., Zhao, L. and Li, J. (2011) A Prediction-Based Handover Trigger Time Selection Strategy in Varying Network Overlapping Environment. 2011 *IEEE Vehicular Technology Conference* (*VTC Fall*), San-Francisco, 5-8 September 2011, 1-5.

[14] Wang, Q. and Ali Abu-Rgheff, M. (2003) A Multi-Layer Mobility Management Architecture Using Cross-Layer Signalling Interactions. 5*th European Personal Mobile Communications Conference*, Glasgow, 22-25 April 2003, 237-241.

[15] Yoo, S.J., Cypher, D. and Golmie, N. (2010) Timely Effective Handover Mechanism in Heterogeneous Wireless Networks. *Wireless Personal Communications*, **52**, 449-475. http://dx.doi.org/10.1007/s11277-008-9633-8

[16] Salih, Y.K., See, O.H. and Yussof, S. (2012) A Fuzzy Predictive Handover Mechanism Based on MIH Links Triggering in Heterogeneous Wireless Networks. *International Proceedings of Computer Science & Information Technology*, **41**, 225.

[17] Liang, X., Li, X., Shen, Q., Lu, R., Lin, X., Shen, X. and Zhuang, W. (2012) Exploiting Prediction to Enable Secure and Reliable Routing in Wireless Body Area Networks. 2012 *Proceedings IEEE INFOCOM*, 25-30 March 2012, 388-396.

[18] Guan, Q., Yu, F.R., Jiang, S. and Wei, G. (2010) Prediction-Based Topology Control and Routing in Cognitive Radio Mobile Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*, **59**, 4443-4452. http://dx.doi.org/10.1109/TVT.2010.2069105

[19] Alavi, B. and Pahlavan, K. (2006) Modeling of the TOA-Based Distance Measurement Error Using UWB Indoor Radio Measurements. *Communications Letters*, **10**, 275-277. http://dx.doi.org/10.1109/LCOMM.2006.1613745

[20] Ravi, R.J. and PonLakshmi, R. (2013) A New Lifetime Prediction Algorithm Based Routing for VANETs. *International Journal of Computer Science & Applications* (*TIJCSA*), **1**, 72-78.

[21] Sharma, A.K. and Parihar, P.S. (2013) An Effective DoS Prevention System to Analysis and Prediction of Network Traffic Using Support Vector Machine Learning. *International Journal of Application or Innovation in Engineering & Management*, **2**, 249-256.

[22] Wu, J., Liu, S., Zhou, Z. and Zhan, M. (2012) Toward Intelligent Intrusion Prediction for Wireless Sensor Networks Using Three-Layer Brain-Like Learning. *International Journal of Distributed Sensor Networks*, **2012**, 243841. http://dx.doi.org/10.1155/2012/243841

[23] Maei, H.R., Szepesvari, C., Bhatnagar, S., Precup, D., Silver, D. and Sutton, R.S. (2009) Convergent Temporal-Difference Learning with Arbitrary Smooth Function Approximation. *Proceedings of the* 23*rd Annual Conference on Neural Information Processing Systems* (*NIPS*'09), Vancouver, 7-10 December 2009.

[24] Eik Loo, C., Yong Ng, M., Leckie, C. and Palaniswami, M. (2006) Intrusion Detection for Routing Attacks in Sensor Networks. *International Journal of Distributed Sensor Networks*, **2**, 313-332. http://dx.doi.org/10.1080/15501320600692044

[25] Chen, C., Ma, J. and Yu, K. (2006) Designing Energy-Efficient Wireless Sensor Networks with Mobile Sinks. *Proceeding of the* 4*th ACM Conference on Embedded Networked Sensor Systems* (*SenSys* 2006), Colorado, 31 October-3 November 2006.

[26] Yan, K.Q., Wang, S.C. and Liu, C.W. (2009) A Hybrid Intrusion Detection System of Cluster-Based Wireless Sensor Networks. *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong, 18-20 March 2009, 18-20.

[27] Shen, W., Han, G., Shu, L., Rodrigues, J.J. and Chilamkurti, N. (2012) A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, **51**, 1-12.