2016 IEEE Mobile Computing PROJECT LIST BASED ON NS2

1. **Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes**
With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Over the years, emphasis has also been placed on improving the security of these networks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation, we demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable. Last, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

2. **Performance Evaluation of Manet Using Quality of Service Metrics.**

An ad hoc network is a collection of mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Several routing protocols have been proposed for ad hoc networks and prominent among them are Ad hoc On Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR). Effort has been made to merge software Quality assurance parameters to adhoc networks to achieve desired results. This Paper analyses the performance of AODV and DSR routing protocols for the quality assurance metrics. The performance differentials of AODV and DSR protocols are analyzed using NS-2 simulator and compared in terms of quality assurance metrics applied.

3. Behavior Malware Detection in Delay tolerant Sensor N/W

The delay-tolerant-network (DTN) model is becoming a viable communication alternative to the traditional infrastructural model for modern mobile consumer electronics equipped with short-range communication technologies such as Bluetooth, NFC, and Wi-Fi Direct. Proximity malware is a class of malware that exploits the opportunistic contacts and distributed nature of DTNs for propagation. Behavioural characterization of malware is an effective alternative to pattern matching in detecting malware, especially when dealing with polymorphic or obfuscated malware. In this paper, we first propose a general behavioural characterization of proximity malware which based on Naive Bayesian model, which has been successfully applied in non-DTN settings such as filtering email spams and detecting botnets. We identify two unique challenges for extending Bayesian malware detection to DTNs (“in sufficient evidence vs. evidence collection risk” and “filtering false evidence sequentially and distributedly”), and propose a simple yet effective method, look-ahead, to address the challenges. Furthermore, we propose two extensions to look-ahead, dogmatic filtering and adaptive look-ahead, to address the challenge of “malicious nodes sharing false evidence”. Real mobile network traces are used to verify the effectiveness of the proposed methods

4. Efficient and Consistent Path Loss Model for Mobile Network Simulation

The accuracy of wireless network packet simulation critically depends on the quality of wireless channel models. Path loss is the stationary component of the channel model affected by the shadowing in the environment. Existing path loss models are inaccurate, require excessive measurement or computational overhead, and/or often cannot be made to represent a given environment. This paper contributes a flexible path loss model that uses a novel approach for spatially coherent interpolation from available nearby channels to allow accurate and efficient modeling of path loss. We show that the proposed model, called Double Regression (DR), generates a correlated space, allowing both the sender and the receiver to move without abrupt change in path loss. Combining DR with a traditional temporal fading model, such as Rayleigh fading, provides an accurate and efficient channel model that we integrate with the NS-2 simulator. We use measurements to validate the accuracy of the model for a number of scenarios. We also show that there is substantial impact on simulation behavior when path loss is modeled accurately. Finally, we show that unlike statistical models, DR can make a simulation representative of a given environment by using a small number of seeding measurements. Thus, DR provides a cost-effective alternative to ray tracing or detailed site surveys.

5. STARS: A Statistical Traffic Pattern Discovery System for MANETs

Many anonymity enhancing techniques have been proposed based on packet encryption to protect the communication anonymity of mobile ad hoc networks (MANETs). However, in this paper, we show that MANETs are still vulnerable under passive statistical traffic analysis attacks. To demonstrate how to discover the communication patterns without decrypting the captured packets, we present a novel statistical traffic pattern discovery system (STARS). STARS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. STARS is capable of discovering the sources, the destinations, and the end-to-end communication relations. Empirical studies demonstrate that STARS achieves good accuracy in disclosing the hidden traffic patterns.

6. Zone based node replica detection using trust values

Wireless sensor networks (WSN) are susceptible to various kinds of attack, and node replication attack is one of them. It is considered to be one of the most serious attacks in WSN. In this type of attack, an adversary deploys clones of a legitimate node. These clones participate in all network activities and behave identically same as the legitimate node. Therefore, detection of clones in the network is a challenging task. Most of the work reported in the literature for clone detection is location dependent. In this paper, we have proposed a location independent zone-based node replica detection technique. In the proposed scheme, the network is dynamically divided into a number of zones. Each zone has a zone-leader, and they share their membership list among themselves. It is the responsibility of the zoneleader to detect the clone. The proposed technique is a deterministic one.We have compared our scheme with LSM, RED, and P-MPC and observed that it has a higher clone detection probability and a lower communication cost.