Theory of Automata Report

Group Members:

i) Bilal Ahmed Khan (20K-0183)
ii) Mohammad Wamiq Akram (20K-1857)
iii) Zulnoor Siddiqui (20K-1090)

Report Submitted to:

Sir Musawar Ali

Contents

1. Introduction

This report analyzes 2 research papers on the Applications of Finite State Machines in Mobile Networks. Mobile Networks/ wireless telecommunication is an ever-growing field in the world of today which is more connected than ever before.

Like every rapidly advancing sector Mobile Networks also faces a number of challenges such as secure transfer of data, growing privacy concerns among the masses, developing less power consuming mobile networks which can help people to communicate in remote areas.

Finite State Machines play a special role in the field of Mobile Networking, from developing complex working model for gathering meaningful information for helping researchers, developing new and more efficient communication protocols, and securing lines of communication to allow the users of the mobile network care free without having them being worrying about the security of the network.

Below we analyze a number of research papers outlining how Finite State Machines play a key-role in different branches of Mobile Networking.

2. Application of Finite Machines in Mobile Networks

a. Finite State Machines: Preserving Privacy When Data-Mining Cellular Phone Networks

Abstract:

Owing to the recent advancements in the telecommunications sectors, researchers are now using telecommunications data from cellular networks. However, the use to user data from Cellular data poses new and difficult questions which require to maintain the balance between personal privacy and public good. This article proposes a unique solution to this intriguing problem, i.e. the use of Finite state Machines which as a technique is particularly suited to the specific computational and technical constraints of a cellular network. This approach allows the users to maintain their privacy while allowing the researchers to go forward by making the relevant data accessible to them.

Privacy Issues:

Not long ago, due to the expensive price of hardware it was quite difficult to keep track of an individual’s digital whereabout using telecommunications. But due to the rapid advancements in the field of telecommunications and IT, it has now become possible readily keep track of virtually every person connected to the internet.

Readily available cellular data has made it possible to calculate preferred routes and destinations, the mode of transports (public or private) and broadly determining how humans interact with each other in this day and age. Although the use of cellular data for these purposes has a number of advantages but there is growing public concern over the use and misuse of personal cellular data for the kind of research that makes all these innovations possible.

One major issue about determining the privacy of individual upon cellular data is that its highly contextual, for example: people expect different levels of personal privacy when say, they are in a public place or inside their home. Hence, its quite difficult to lay out a uniform policy to determine what kind of collection of cellular data is ethical and what is the limit when it intrudes a user’s personal privacy.

Finite State Machines and Privacy Management:

Finite State Machines share a lot of features with geographical agent based models. As a matter of fact, Finite State Machines have been embedded in many computer applications ranging from artificial intelligence research to Video games.

In its simplest form, a finite state machine is built on two components: states and actions.

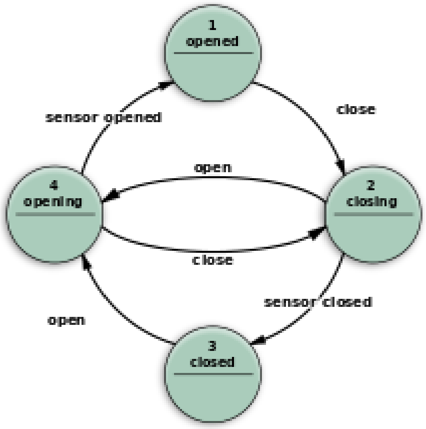


Figure 1 A simple finite state machine

When an action happens, it brings some kind of change in the state of the subject which in turn can make the subject to do new actions. Basing our machines on these simple rules we can create very complex systems to perform a variety of tasks. The actions in a Finite State Machine have four different sub-classes: entry, exit, input and transition. The Input induces a subject to bring about a change in its state, the subject performs the entry action when it enters the new state and the transitions occurs when the subject is moving from one state to another.

Finite state machine models can be used to securely collect data from the users, consider the example of a targeted campaign being run by a company in a known radius. When a user who has a cell phone enters the radius, the cellphone connects to the communication tower and receives a notification in the form of an offer form the company, the user can opt to proceed and take further actions or deny the offer. In the case of denial the user is dropped from the network and no further information is gathered related to the user, such a state is called a "dead state" in the FSM models. These models prove to be more efficient than collecting data of all the customers with in a given area because FSM machines filter out those who are not interested in the product/survey allowing researchers/ companies to focus on their target demographic/focus group.

Proposed Solution:

Implementation of FMS models on a large scale can prove to be very beneficial for companies as well as researchers on a large scale. Since it enables the researches to implement a number of privacy-focused techniques which do not require much technically sophisticated equipment, enabling the researchers to get access to valuable data without compromising on the privacy of individuals.

b. Computation Termination and Malicious Node Detection using Finite State Machine in Mobile Ad hoc Networks (MANETs)

Abstract:

The wireless tech has grown tremendously over the past two decades, with new innovations and exciting advancements in the networking domains with every passing day. Mobile Ad hoc Networks (MANETs) is one such alluring advancement of the recent era in which the participating nodes of the network do not require any active, existing or centralized system/rigid infrastructure for executing their purpose and thus they possess the moving capability on arbitrary basis. In MANETs for those within range the radio range nodes communicate with each other directly while relay principle for communication is used by outside nodes.

Although MANETS offer a highly cost-effective solutions compared to contemporary technologies because of their non-reliance on rigid infrastructure but security is a major concern barring its use in the mainstream. Moreover, limited energy reserve, resource constraints and high dynamic topology which render them more vulnerable compared to wired networks. This research paper primarily focuses on the use of Finite State Machines for the computation termination of cluster head algorithm and also for identification of malicious nodes on the MANET.

Route Discovery and Maintenance:

MANETs have spread rather quickly in a number of areas of wireless domains, owing to the enormous growth of MANETs in almost every field of networking the serve to be a good candidate for gathering data by the researchers but still they find it difficult to incorporate MANETs in their research flow due to a number of reasons.

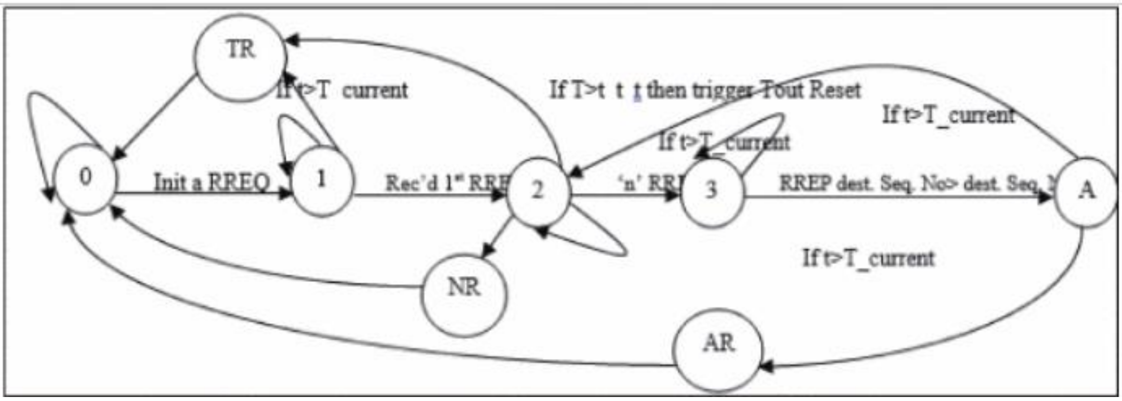
The use of FINITE MACHINES can allow the researches to overcome the existing hurdles faced by researches and open new avenues in the field of networking. Currently MANET networks are highly recognized being based upon the 802.11 (Wi-Fi) Family. MANET in itself, is a self responsive and directed system in which wireless nodes communicate with each other and do not require any other infrastructure. Since all the nodes on a MANET network are decentralized they are bound to take a self determined route for routing, this vulnerability is a major cause of concern for MANET users. Analysis of Data of the past decade has shown that engagement, globalization and involvement of attacks has enormously been inflated leading to the exploitation of a MANET network by potential attackers.

Since nodes in the network are self-directed, to send a message a node determines its own path to send the information form the source to its destinations, to do this RREQ(Route Request) along with setting a timer for RREP (Route Reply) message. If the route is accessible then the communication takes place otherwise the node initiates a route discovery request.

Due to the power and computational constraints of MANETs a node may decide to participate or not participate in the process of routing to preserve its energy and act selfishly. Thus, the packet which was not intended for itself may end up dropping it from the malevolent node causing a network segmentation. A malicious node on the network may take advantage of this behavior and convert all the rest of the participating nodes into promiscuous nodes causing the network to behave in unintended behavior.

Finite State Machines can be used to overcome this vulnerability in MANETs, the FSM enters the pre-alarm state for t seconds if the node does not succeed with the forwarding request. Consequently the machine resets itself to the normal state not allowing the malicious node to take control of the network hence keeping the network secure from a number of attacks.

The FSM diagram below show a practical demonstration about the mechanism of the FSM.



Prospect Work and Possible Solutions:

MANET is one of the most promising research area in the networking field with major practical based applications. But due to its decentralized nature and lack of security provisions it becomes susceptible to all types of attacks. The use of FSM models can prove to be a major breakthrough in this regard, rectifying the security vulnerabilities of MANETs and making them suitable for large scale mainstream research and other purposes.

3. Citations

a. Jonathan Reades (2010) Finite State Machines: Preserving Privacy When Data-Mining Cellular Phone Networks, Journal of Urban Technology, 17:1, 29-40, DOI: 10.1080/10630731003597314

b. S. V. Sonekar, M. Pal, M. Tote, S. Sawwashere and S. Zunke, "Computation Termination and Malicious Node Detection using Finite State Machine in Mobile Adhoc Networks," 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), 2020, pp. 156-161, doi: 10.23919/INDIACom49435.2020.9083710.