IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 3 (Sep-Oct. 2012), PP 15-24
www.iosrjournals.org

Mobile Networking and Ad hoc routing protocols validation

[1]Simanta Sarma, [2]Dr. Sarbananda Das
[1](HOD & Asstt. Professor, Department of Computer Science, S.B.M.S College, Sualkuchi, Assam, India)
[2](Rtd. Principal, North Gauhati College, North Guwahati, Assam, India)

Abstract: *In this paper we describe mobile network and efficient routing protocol for wireless ad hoc networks. We report on its implementation, on performance comparisons and on a formal validation result. Moreover we discuss Cellular system design, global System for mobile Communication, Formal Protocol Verification and operating over infrared or Bluetooth. This paper evaluates two model checking tools, SPIN and UPPAAL, using the verification of the Ad hoc Routing protocol as a case study. Insights are reported in terms of identifying important modeling considerations and the types of ad hoc protocol properties that can realistically be verified.*

Keywords*.: Cellular Phone network, mobile ad hoc networks, routing protocols, Wireless networks, ad hoc routing, routing protocol Implementation, formal validation, model checking, Infrared or Bluetooth, GSM.*

I. Introduction

Cellular communications has experienced explosive growth in the past two decades. Today millions of people around the world use cellular phones. In modern area Cellular phones are most important factor in human life. Cellular phones allow a person to make or receive a call from almost anywhere. Likewise, a person is allowed to continue the phone conversation while on the move. Cellular communications is supported by an infrastructure called a cellular network, which integrates cellular phones into the public switched telephone network. Cellular service has seen tremendous acceptance, especially in the last few years, with millions of new subscribers each year and the new subscriber rate growing. Some estimates predict that half a billion cellular phones will be in service by the end of the next decade. AD-HOC networks are typically described as a group of mobile nodes connected by wireless links where every node is both a leaf node and a router. For a cellular system the major resources available are:

1. Bandwidth
2. Power

Out of which bandwidth is a major issue of concern. Because the spectrum allocated for cellular communication is limited. With the great increase in number of wireless devices such as mobile phones, the demand for wireless communications has grown exponentially over the last decade and is expected even more in the future. More and more multimedia traffic are being transmitted via wireless media, and such applications require diverse QoS. Hence there is scarcity of bandwidth. High-speed cellular networks working today are expected to support multimedia applications, which require QoS provisions. Since frequency spectrum is the most expensive resource in wireless networks, it is a challenge to support QoS using limited frequency spectrum.

II. Mobile Ad-Hoc Network

Theoretical mobile ad hoc networking research [CCL03] started some decades ago. But commercial digital radio technologies appeared in the mid-nineties. Since then, few proposals for enabling ad hoc communications were made. The first technology (IEEE802.11, also referred to as Wi-Fi [ANS99]) is still strongly leading the market, although there is great room for improvement. This section provides an overview and a technical description of the technologies that have been proposed hitherto. A common feature of most wireless networking technologies is that they operate in the unlicensed Industrial Scientific and Medical (ISM) 2.4GHz band. Because of this choice of frequency band, the network can suffer interferences from microwave ovens, cordless telephones, and other appliances using this same band plus, of cours, other networks. In particular, Farrell and Abukharis studied the impact on Bluetooth on IEEE802.11g [ST04]

2.1 Packet radio

Packet radio [GFS78] was used for the earliest versions of mobile ad hoc networks. It was sponsored by DARPA in the 1970s. It allows the transmission of digital data over amateur radio channels. Using special radio equipment, packet radio networks allowing transmissions at 19.2 kbit/s, 56 kbit/s, and even 1.2 Mbit/s have been developed. Since the modems employed vary in the modulation techniques they use, there is no standard for the physical layer of packet radio networks. Packet radio networks use the AX.25 data link layer protocol, derived from the X.25 protocol suite and designed for amateur radio use. AX.25 has most frequently been used to establish direct, point-to point links between packet radio stations, without any additional network

layers. However, in order to provide routing services, several network layer protocols have been developed for use with AX.25. Most prominent among these are NET/ROM, ROSE, and TexNet. In principle, any network layer protocol may be used, including the Internet protocol (IP), which was implemented in the framework of the AMPRNet project.

2.2 IEEE802.11

Wi-Fi is a wireless networking technology based on the IEEE802.11 specifications. The first—and still most used—Wi-Fi standard is referred to as IEEE802.11b in the scientific literature. It was then declined into IEEE802.11a, IEEE802.11g and IEEE802.11n. IEEE802.11i and IEEE802.11h, which respectively focus on Quality of Service (QoS) and security, are out of the scope of this document. All Wi-Fi technologies operate on the 2.4GHz band, except from IEEE802.11a which operates within the 5GHz band. These technologies use significantly different PHY layers which, from the user point of view, make them differ in term of the bandwidth (i.e. the data rate) that they provide. Typically, Wi-Fi enabled devices have coverage distances ranging from 50 to more than 100 meters. In practice, this coverage distance depends greatly on the nature of the antenna and on the environment in which the devices evolve.

2.2.1 IEEE802.11a

IEEE802.11a uses Orthogonal Frequency Division Multiplexing (OFDM). It is the only wireless radio technology that works in the 5GHz band. The main idea behind OFDM is that since low-rate modulations (i.e modulations with relatively long symbols compared to the channel time characteristics) are less sensitive to multipath, it should be better to send a number of low rate streams in parallel than sending one high rate waveform. OFDM then works by dividing one high-speed signal carrier into several lower-speed subcarriers, which are transmitted in parallel. High-speed carriers, which are 20MHz wide, are divided into 52 sub channels, each approximately 300KHz wide. OFDM uses 48 of these sub channels for transporting data, while the four others are used for error correction. OFDM delivers higher data rates and a high degree of multipath reflection reconstruction, thanks to its encoding scheme and error correction.

2.2.2 IEEE802.11b

IEEE 802.11b uses Direct Sequence Spread Spectrum (DSSS) as the physical layer technique for the standard. DSSS uses a complex technique which consists in multiplying the data being transmitted by a *noise* signal. This noise signal is a pseudo-random sequence of 1 and −1 values, at a frequency much higher than the original signal. The resulting signal wave looks much like white noise. This white noise can be filtered at the receiving end in order to recover the original data. This filtering happens by again multiplying the same pseudo-random sequence by the received signal (because $1 \times 1 = 1$, and $-1 \times -1 = 1$). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted pseudo-random sequence with the receiver's assumed sequence. For allowing de-spreading to work correctly, the transmit and received sequences must *synchronized*. So far, IEEE 802.11b is the implementation of the IEEE 802.11 standard that has been most heavily studied in the framework of mobile ad hoc networks.

2.2.3 IEEE802.11g

IEEE802.11g, just like IEEE802.11a, uses orthogonal frequency-division multiplexing (OFDM), it then boasts similar bandwidths. OFDM is described in Section 2.2.1. But unlike IEEE802.11a, IEEE802.11g works in the 2.4 GHz band. Since the draft 802.11g standard combines fundamental features from both 802.11a and 802.11b, it leads to the development of devices that can inter-operate with technologies based on both of the previous versions of the specification.

2.3 Bluetooth

Bluetooth is essentially the same kind of microwave radio technology that has given us wireless door chimes and automatic garage door openers. It was initially restricted to an operating distance of just 10 meters and a speed of approximately 1 Mbit/s. When Bluetooth devices come within range of each other, they establish contact and form a temporary network called a Personal Area Network (PAN). In the Bluetooth terminology, this is also known as a Piconet. A multi-hop ad hoc network formed by the interaction of Bluetooth devices is called a Scatternet. When using Bluetooth, the devices must establish a network session before being able to transmit any data. Bluetooth uses the Frequency-Hopping Spread Spectrum (FHSS) technique. Unlike IEEE802.11 which establishes a communication link on a certain frequency (a channel), FHSS breaks the data down into small packets and transfers it on a wide range of frequencies across the available frequency band. Bluetooth transceivers jump among 79 hop frequencies in the 2.4 GHz band at the rate of 1,600 frequency hops per second. 10 different types of hopping sequences are defined, 5 of the 79 MHz range/79 hop system and 5 for the 23 MHz range/23 hop system.

This technique trades off bandwidth, in order to be robust and secure. More precisely, Spread Spectrum communication techniques have been used for many years by the military because of their security capabilities.

2.4 Hiperlan

The HiperLAN2 standard is very close to 802.11a/g in terms of the physical layers it uses—both use OFDM technology—but is very different at the MAC level and in the way the data packets are formed and devices are addressed. On a technical level, whereas 802.11a/g can be viewed as true wireless Ethernet, HiperLAN2 is more similar to wireless Asynchronous Transfer Mode (ATM). It operates by sharing the 20MHz channels in the 5GHz spectrum in time, using Time Division Multiple Access (TDMA) to provide QoS through ATM-like mechanisms. It supports two basic modes of operation: centralized mode and direct mode. The centralized mode is used in the cellular networking topology where each radio cell is controlled by an access point covering a certain geographical area.

2.5 ZigBee

ZigBee-enabled devices conform to the IEEE 802.15.4-2003 standard. This standard specifies its lower protocol layers, the physical layer (PHY), and the medium access control (MAC). It targets Low-Rate Wireless Personal Area Network (WPAN). ZigBee-style networks research began in 1998. Zigbee was intended to operate in contexts in which both Wi-Fi and Bluetooth are not suitable. Zigbee operates in the unlicensed 2.4 GHz, 915 MHz and 868 MHz ISM bands. It uses direct-sequence spread spectrum (DSSS) coding. This makes the data rate to reach 250 kbit/s per channel in the 2.4 GHz band, 40 kbit/s per channel in the 915 MHz band, and 20 kbit/s in the 868 MHz band. The maximum output power of ZigBee antennas being generally 1 mW, the transmission range of ZigBee nodes is between 10 and 75 meters. Observations have shown that the transmission range is heavily dependent on the environment.

2.6 Broadband wireless networking

WiMAX (IEEE 802.16) stands for Worldwide Interoperability for Microwave Access. IEEE 802.16 boasts data rates up to 70 Mbit/s over a distance of 50 km. However practical limits from real world tests seem to be between 500 kbit/s and 2 Mbit/s at a distance of around 5-8kms. WiBro is a wireless broadband internet technology being developed by the Korean telecoms industry. It has been announced that WiBro base stations will offer an aggregate data throughput of 30 to 50 Mbit/s and cover a radius of up to 5 km. The technology will also offer Quality of Service.

HIPERMAN [HPF03, HPF04], which stands for High Performance Radio Metropolitan Area Network, is a European alternative to WiMAX. The standards were created by the European Telecommunications Standards Institute (ETSI). It provides a wireless network communication in the 2-11 GHz bands. The adequation of these technologies to ad hoc networking is discussable, since they would permit to establish ad hoc networking at a level at which technologies for infrastructure networks (like GSM or UMTS) are available.

III. Elements Of Cellular System Design

3.1 Frequency Reuse:

Frequency Reuse means, two users in two distant cells can operate on same frequency. The cellular system makes an efficient use of available channels by using low power transmitters to allow frequency reuse at smaller distances. Frequency Reuse can either be in time domain or in frequency domain, it is done by TDMA scheme that is allocation of different time slots to the frequency reuse scheme. In frequency domain, it is done by FDMA scheme, i.e. repeat carrier frequency after some time and frequency reuse distance.

3.2 Frequency Reuse Distance (D):

It means the minimum distance which allows the same frequency to be reused

$$D = R\sqrt{3K}$$

K = frequency reuse pattern

$$K = i^2 + ij + j^2$$

R = radius of the cell

3.3 Call Blocking Probability:

Blocking probability is the probability of blocking calls out of N number of calls generated in a busy hour condition. It is measured in Erlangs.

3.4 Co-channel Interference Ratio:

The *S/I* ratio at the desired mobile receiver is given as:

$$\frac{S}{I} = \frac{S}{\sum_{k=1}^{N_I} I_k}$$

Where:
Ik = the interference due to the *k*th interferer
NI = the number of interfering cells in the first tier.

In a fully equipped hexagonal-shaped cellular system, there are always six Co-channel-interfering cells in the first tier (i.e., *NI* = 6, see Figure 2.7). Most of the co-channel interference results from the first tier. Contribution from second and higher tiers amounts to less than 1% of the total interference and, therefore, it is ignored. Co-channel interference can be experienced both at the cell site and the mobile stations in the center cell. In a small cell system, interference will be the dominating factor and thermal noise can be neglected. Thus the *S/I* ratio can be given as:

$$\frac{S}{I} = \frac{1}{\sum_{k=1}^{6} \left(\frac{D_k}{R} \right)^{-\gamma}}$$

where:
$2 \leq \gamma \leq 5$ = the propagation path loss, and _ depends upon the terrain environment
Dk =the distance between mobile and *k*th interfering cell, *R* = the cell radius

IV. Global System For Mobile Communication (GSM)

GSM (Global System for Mobile communications): is the most popular standard for mobile phones in the world. The GSM Association estimates that 80% of the global mobile market uses the standard. GSM is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band. Mobile services based on GSM technology were first launched in Finland in 1991. GSM, together with other technologies, is part of the evolution of wireless mobile telecommunications that includes High-Speed Circuit-Switched Data (HCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS).

4.1 GSM SYSTEM ARCHITECTURE:

- **Mobile Station (MS)**
  - Mobile Equipment (ME)
  - Subscriber Identity Module (SIM)
- **Base Station Subsystem (BSS)**
  - Base Transceiver Station (BTS)
  - Base Station Controller (BSC)
- **Network Switching Subsystem(NSS)**
  - Mobile Switching Center (MSC)
  - Home Location Register (HLR)
  - Visitor Location Register (VLR)
  - Authentication Center (AUC)
  - Equipment Identity Register (EIR)

GSM ARCHITECURE DIAGRAM:

Interfaces:
Um= Interface between MS and BTS.
Abis= Interface between BTS and BSC.
A= Interface between BSC and MSC.
B= Interface between MSC and VLR.
C= Interface between GMSC and HLR.
D= Interface between VLR and HLR.
E= Interface between MSC and other MSC.
F= Interface between MSC and EIR.
G= Interface between VLR and other VLR**.**

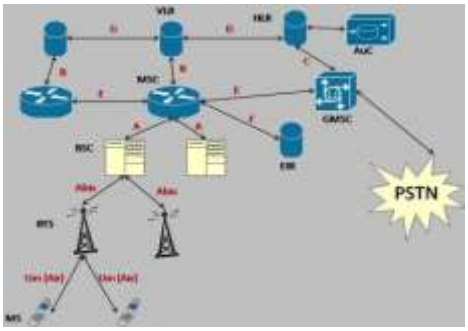

Figure1:GSM architecture

a) Mobile Station (MS):
The Mobile Station is made up of two entities:

1. Mobile Equipment (ME) :

It is a portable, vehicle mounted or handheld device. It is uniquely identified by IMEI (International Mobile Equipment Identity).

Functions:

1. It monitors power and signal quality of surrounding cells for optimum handover.
2. Used for voice and data transmission.

2. Subscriber Identity Module (SIM)

In the GSM Network, the SIM card identifies the user. The SIM is a small memory device, which contains the identification numbers of the user (IMSI) and a list of available networks .The SIM card also contains tools needed for authentication and ciphering.

4.2 MULTIPLE ACCESS TECHNOLOGIES

4.2.1 Frequency Division Multiple Access (FDMA):

In the FDMA system, one specific frequency is allocated to one user engaged in a call. When there are numerous calls, the network tends to get overloaded, leading to failure of the system. In a full-rate (FR) system, eight time slots (TS) are mapped on every frequency, while in the half-rate (HR) system, sixteen TSs are mapped on every frequency (Figure 2).

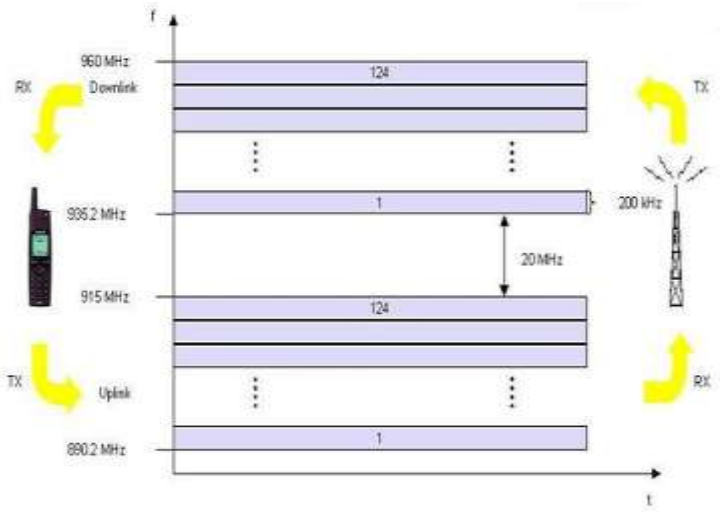

Figure 2: FDMA

4.2.2 Time Division Multiple Access (TDMA) :

TDMA systems divide whole transmission time into time slots, and in each slot only one user is allowed to either transmit or receive. TDMA shares a single carrier frequency with several users, where each user makes use of non-overlapping time slots. Each TRX handles one carrier frequency and can be a hopping carrier frequency or a fix carrier frequency. If the carrier frequency is hopping it continuously changes between different radio frequencies. This is done to reduce the interference with other channels and cells (Figure 3).

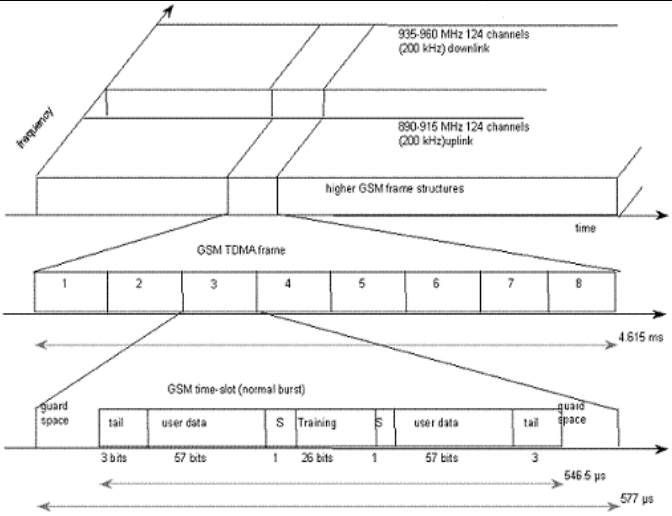

Figure 3:TDMA

In order to multiply users per carrier frequency the GSM uses Time Division Multiple Access (TDMA). The TRXs divides the time in 8 Time Slots (TS) of a length of approximately 0.577ms. Very simplified you can say that one user uses one time slot to make a call in GSM. One period of 8 TSs is called a TDMA Frame and has the length of approximately 4.615 ms. In each cell one of the TRXs, called C0 has to configure one of its TSs to the Broadcast Control Channel (BCCH) and is not allowed to hop, this TS is referred to as TS0. A TS configured to carry the BCCH cannot be used for speech or data sessions. Due to frequency hopping the rest of the TSs of the TDMA Frame can be able to use frequency hopping depending on what technique is used. Each TS on a TDMA frame is referred to as a physical channel.

4.2.3 Code Division Multiple Access (CDMA) :

Code-division multiple access combines modulation and multiple access to achieve a certain degree of information efficiency and protection. Initially developed for military applications, it gradually developed into a system that gave the promise of better bandwidth and service quality in an environment of spectral congestion and interference.

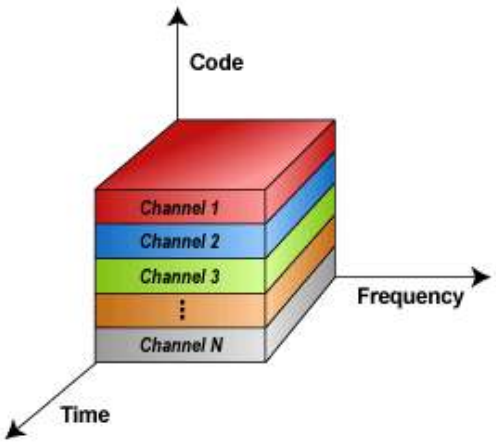

Figure 4:CDMA

In this technology, every user is assigned a separate codes depending upon the transaction. One user may have several codes in certain conditions. Thus, separation is not based on frequency or time, but on the basis of codes. These codes are nothing but very long sequences of bits having a higher bit rate than the original information. The major advantage of using CDMA is that there is no plan for frequency refuse, the number of channels is greater, there is optimum utilization of bandwidth, and the confidentiality of information is well protected (Figure 4).

4.3 LOGICAL CHANNELS IN GSM NETWORK:

Fig 5 channels in GSM network

4.3.1 Traffic Channels (TCH) –

TCH transport user information (speech/data)

- TCH are bidirectional dedicated channels between the network and the MH

4.3.2 Broadcast Channels (BCH)

-To help the MH (Mobile Handset) measures

- to turn to a BTS
- to listen for the cell information
- to start roaming, waiting for calls to arrive, making calls
- Because BTSs are not synchronized with each other, every time a MH decides to camp to another cell, its FCCH, SCH, and BCCH must be read.

4.3.3Common Control Channels (CCCH)

CCCH support the establishment of a dedicated communication path (dedicated channel) between the MH and the BTS. Three types of CCCH

1. Paging Channel (PCH)
2. Random Access Channel (RACH)
3. Access Grant Channel (AGCH)

4.3.3.1Paging Channel (PCH)

-Used by BTS to page particular MH in the cell
-MH actively listen to PCH to check contact information within certain time
-Contact could be incoming call or short message
-Contact information on PCH include
-IMSI (MH's identity number), or TMSI (temporary number)
-Transmit on down-link , point to point

4.3.3.2Access Grant Channel (AGCH)

-The network assigns a signaling channel via AGCH
-A Stand alone Dedicated Control Channel (SDCCH) is assigned
-Transmit on down-link, point to point

4.3.3.3Random Access Channel (RACH)

-Used by MH to request a dedicated channel for call setup
-Shared by any MH attempts to access the network
-Channel request message contains the reason for the access attempt
-Transmit on up-link , Point to point

4.3.4 Dedicated Control Channels (DCCH)

DCCH are used for transferring nonuser information between the network and the MH Messages on DCCH Including

-channel maintenance
-mobility management

Four kinds of DCCH

1. Stand alone Dedicated Control Channel (SDCCH)
2. Cell Broadcast Channel (CBCH)
3. Slow Associated Control Channel (SACCH)
4. Fast Associated Control Channel (FACCH)

V. Protocol Validation

5.1 Survey of Methods

Computer networking protocol validation is commonly done using a combination of simulation and testing. These are both valid approaches that to some extent complement each other. Simulation offers the possibility to run a large batch of tests under identical circumstances whereby some parameter can be varied and

the effect studied. A very common assisting tool, or framework, is the network simulator - ns-2 [26]. Live testing is often applied to some extent during protocol development. An important application for the method is when checking interoperability between different implementations. Live testing poses the difficulty of conducting several comparable tests, but if done in a structured way it may very well expose errors or problems not visible in simulations. The gray zone problem, reported by Lundgren et al. [34] is one example of such a discrepancy. In Paper C initial results from a structured live testing study are presented. The tool we use is called the APE testbed [38]. A third alternative is to use formal verification in order to be sure to cover all situations possible in a system model. Testing and simulation are not exhaustive methods and cannot guarantee that there are no undiscovered subtle errors or design flaws in a protocol. The objective of formal verification is to improve on reliability by reasoning about systems using mathematical logic. A formal system model can thereby be checked to fully comply with a given set of requirements. There have been comparatively few efforts at formal verification of ad hoc routing protocols. The reason for this is twofold. First, there is the presumption that the methods are difficult to use which is to some extent
true since there really is a threshold to cross before becoming proficient. The deductive methods usually require more experience before it is possible to carry out a proof for a non trivial system. Even then, it is often a very time consuming process.

In the case of deductive methods they have a potential to be very powerful and can be used to construct proofs for large or even infinite state systems. However, the proof may be notoriously difficult to find or it may not even exist because the problem is not well formulated. Algorithmic verification methods, commonly known as model checking [9], have been more successful in terms of industrial deployment because of their easier usage. These methods have another problem that surfaces for systems composed from a set of different components that can interact in a non deterministic manner. Many possible interleavings of execution are thereby possible, leading to exponential growth of the searched state space; the state explosion problem [47]. These new techniques thus have the potential for verifying infinite state systems automatically by abstract interpretation [15] followed by, for example, symbolic model checking [36]. There is ongoing work on many fronts in order to lower the threshold of use as well as on coping with the state explosion problem. Here, we concentrate on some of the more user friendly tools, namely automatic model checkers. Our hope is to advocate the use of formal verification by the average protocol designer.

5.2 Formal Protocol Verification

5.2.1 System Description Languages

In order to verify a particular protocol it first has to be described in a structured and unambiguous way. For this, there are two main choices. Either, one can write an implementation in a regular programming language such as C and thereafter verify the code directly. This approach has been used by Engler and Musuvathi [18] to find errors in different AODV implementations. It is most often not used for exhaustive verification but rather as a method of finding program bugs, even though Engler and Musuvathi were also able to identify a routing loop error in the AODV specification. The second approach to describing the protocol is to use a formal description language. This can either be a subset of first order predicate logic or some more high level formalism such as PROMELA (PROcess Meta LAnguage) used in the SPIN [23] tool. In reality, these languages are just representations of transition systems. It is essential that the formal description matches that of the real system implementation, but normally some parts have to be abstracted away from in order to make the problem feasible for verification. In the case of deductive verification the proof may otherwise be too difficult to construct and in the case of model checking the state space can easily blow up. When abstracting, one has to make sure that the system model retains the same behavior as the implementation for the properties of interest.

Table 1. SPIN verification results

Scenario	States generated	Transitions	All states searched	Memory used [Mb]	Time used
(a)	5715	12105	Yes	4.242 (6.188)	0.20 (0.20) s
(b)	269886	731118	Yes	33.05 (124.7)	12.33 (10.48) s
(c)	53614	128831	Yes	8.836 (30.12)	2.19 (1.92) s
(d)	4.58e+07 (8.15e+06)	1.33e+08 (2.21e+07)	No	4083 (4083)	5 h:57 min (8 min:56 s)
(e)	1.41e+06	4.59e+06	Yes	170.4 (806.6)	1:36 (1:26) min:s
(f)	3.40e+07 (7.27e+06)	1.22e+08 (2.50e+07)	No	4083 (4083)	4 h:2 min (9 min:43 s)

5.2.2 Requirement Properties and Specification Languages

Requirements on the system are commonly expressed in a temporal logic such as LTL (Linear Temporal Logic) [43] or CTL (Computation Tree Logic) [10]. Requirement properties can be categorized as either liveness or safety properties [29]. Characteristic for a safety property is that a violation is detectable using a finite system run. It can informally be described using the sentence "something bad will never happen" provided that the property holds in all reachable system states. In contrast, a liveness property corresponds to the sentence "something good will eventually happen". In order to produce a counter example for a liveness property it is sometimes necessary to study infinite system runs. An example of a liveness property is the one we used in Paper B and Paper D, expressed somewhat simplified: under the appropriate premises, a given routing protocol will eventually find a route to a particular destination.

5.2.3 Applying the Method

5.2.3.1. Model Checking

There are two main advantages of model checking in comparison to deductive methods. The first one is that once the system model has been constructed and the verification properties devised, the process is completely automatic and outputs a "yes" or "no" answer. The other advantage is the possibility to generate error traces in case a property is not fulfilled by the system. This makes it possible for the user to modify the model accordingly. The main disadvantage of model checking is its limitation to finite state systems. It can, however, be used in hybrid infinite state verification approaches where model checking is, for example, a component in a CEGAR (Counter-Example Guided Abstraction Refinement) loop [12]. Furthermore, model checking of symbolically represented systems can be regarded as infinite state since the original system may contain an unlimited element (such as continuous time). Using model checking, one can check safety as well as liveness properties. Model checking algorithms work by exploring the state space whereby the search stops at the first violation or when the complete execution tree has been examined. Methods can be divided into explicit state and symbolic model checking depending on if the individual states or groups (sets) of states are used to represent the state space.

5.2.3.2Deductive Verification

In deductive verification the goal is to prove that a conclusion, the property to be verified, can be drawn from a given set of premises, the system description. This was previously a tedious manual process which has been speeded up with the emergence of semi-automatic tools, so called theorem provers. One advantage of this method is that it can be used to prove properties of infinite state systems, for example a protocol running in a network with anunbounded number of nodes. An invariant is an assertion that is true in all states of a system. A safety property, expressed as an invariant, can be proven using mathematical induction. First it needs to be proven that the initial system configuration implies the assertion. In the inductive step it is then checked whether all state transitions preserve the property, that is, if the assertion holds before the transition it will also hold after it. Hence, the verification does not require an explicit state space search. This avoids the state explosion problem at the cost of a more cumbersome proof process. The manual method was used by Ogier [40] to make a proof of correctness for the TBRPF [39] protocol. For the discovery module he further presents a proof that the neighbor information exchanged is sufficient for the functionality of the protocol.

5.2.4 The State Explosion Problem and Remedies

The state explosion problem in model checking refers to the situation in which the state space storage overhead grows exponentially with the size of the model. This problem occurs because of the large number of possible interleaving between processes in a reactive concurrent system. Verification may thereby fail simply because the available amount of computer memory is limited. There have been a number of suggestions for coping with the state explosion, that is, to make verification feasible for realistically sized systems. We list the major remedies below following the description by Clarke et al. [9].

Symbolic representation. Symbolic representation refers to the use of compact data structures for representing state space. For example, by encoding the transition relations of a Kripke structure as a Binary Decision Diagram (BDD) it is possible to save storage by exploiting the often inherent regularity of a hardware or software system. Constraint system representation of continuous parameters such as clock ranges, which is done in UPPAAL, is another example of a symbolic representation. In that case it would not even be possible to store all time points explicitly regardless of the amount of available memory.

Partial order reduction. Partial order reduction [24] is an optimization, for example implemented in the SPIN tool. If a group of concurrently executing processes do not exchange any data throughout their lifetime, then it does not make a difference for the end result if they are run one after the other or in parallel. This makes verification simpler since the processes can be verified in isolation. However, once processes cooperate, for example by message passing, which is certainly the case for protocol implementations, then the possible interleaving of operation have to be taken into account when verifying the system. Partial order reduction is a

way of disregarding process interleaving that produce the same global state as some other interleaving. Note that the verification property also needs to be taken into account since it might introduce additional data dependencies between processes. Keeping as much as possible local to each modeled process can thus promote partial order reduction. Compositional reasoning. This technique [2] involves decomposing the system into components which are verified separately and in isolation from the rest. Global properties can then be inferred from the composition of the components. If there are mutual dependencies between components one can still verify each component separately under the assumption that the other components work as expected; assume-guarantee reasoning. There are both manual and automatic approaches available for compositional reasoning.

VI. Related Work

Routing below the IP layer for ad hoc networks was independently adapted by [1] using label switching which is equivalent to the selectors. A similar project is [2] where the authors also aim at putting L2.5 routing logic inside the (wireless) network interface card. For AODV, formal validations have been carried out by the Verinet group [19]. Using a theorem proves and a SPIN model of AODV in a 2 node setup (with an AODV router environment), it is in fact a loop free routing protocol. The Verinet group [23] have carried out formal validation of AODV [13] and identified a flaw that could lead to loop formation. This was done using the HOL [24] theorem prover and a SPIN model of AODV in a two node setup (with an AODV router environment). They have also suggested a modification and verified that, after this, the protocol was loop free. Their approach verified the general case, but the methodology involves substantial user interaction.

VII. Conclusions

This work is to our knowledge the first to study a range of topologies in order to determine where the limit actually is when performing model checking on an ad hoc routing protocol. We have introduced the ad hoc routing protocol which targets the common-case of network clouds with 10-15 nodes and a diameter of up to three hops. We believe that such settings will be the most popular ones where ad hoc networks can and will be put into operation. More specially, in larger settings and for IEEE 802.11 there are such severe degradations occurring under any ad hoc routing scheme that we do not consider this to be a relevant use case that a routing protocol should try to address. When verifying both the data and control aspects of the protocol using SPIN and when verifying the timing properties using UPPAAL the size of network, i.e. the number of nodes involved, as well as the nature of the topological scenarios is limited due to state space storage overhead. Even if parallel model checking approaches were used, our conclusion is that it is at this point not feasible to provide a proof for topologies of any significant size by modeling the protocol directly. On the other hand, our study enables us not only to analyze the modeling considerations that have to be imposed, but also provides us with a solid starting point for the further work we intend to pursue in the direction of infinite-state verification of ad hoc routing protocols.

Acknowledgements:

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank Gauhati University, Assam (Teaching Staff of Department of Computer Science); S.B.M.S College, Sualkuchi, Assam; CMJ University for providing necessary facilities to carry out this work.

References

[1] Bin Li, Lizhong Li, Bo Li and Xi-Ren Cao, "On Handoff Performance for an Integrated Voice/Data Cellular System", Journal of Wireless Networks 9,393-402,2003

[2] Marcos A. C. Lima, Aluizio F.R. Araújo, and Amílcar C. César , **"**Dynamic channel assignment in mobile communications based on genetic algorithm", 0-7803-7589-0/02 2002 IEEE

[3] Somnath Sinha Maha Patra, "Improved Genetic algorithm for channel allocation scheme with channel borrowing in Mobile Computing", IEEE Transactions on Mobile Computing, vol-5, No.7, July 2006.

[4] Arup Acharya, Archan Misra and Sorav Bansal. .A Label-switching Packet Forwarding architecture for Multi-hop Wireless LANs.

[5] Proc WoWMoM'02, Sep 2002, Atlanta, USA Lundgren, H.: Implementation and Real-world Evaluation of Routing Protocols for Wireless Ad hoc Networks. Licentiate thesis, Uppsala University (2002)

[6] IETF MANET Working Group: MANET charter. http://www.ietf.org/html. charters/manet-charter.html (2004

[7] Perkins, C., Belding-Royer, E., Das, S.: Request for Comments: Ad hoc on-demand distance vector (AODV) routing. http://www.ietf.org/rfc/rfc3561.txt (2003).

[8] Johnson, D.B., Maltz, D.A., Hu, Y.C.: Internet draft: The dynamic source routing protocol for mobile ad hoc networks (DSR). http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt (2003).

[9] Xiong, C., Murata, T., Tsai, J.: Modelling and simulation of routing protocol for mobile ad hoc networks using coloured Petri nets. In: Proc. Workshop on Formal Methods Applied to Defence Systems in Formal Methods in Software Engineering and Defence Systems. (2002)

[10] Tian-Tsair SutS, Po-Chiun Huangt, and Chung-Ju Changt,"A channel borrowing protection scheme for handoffs in a cellular based pcs system" , 0-7803-2955-4/95/ IEEE

[11] Holzmann, G.: The Spin Model Checker, Primer and Reference Manual. Addison-Wesley, Reading,Massachusetts (2003)

[12] Barnat, J., Brim, L., Stribrna, J.: Distributed LTL model-checking in SPIN. Technical Report, Masaryk University (2000)