Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Rural Communication Enhancement Using Mobile Ad-Hoc Network

[1]Suman Bajaj, [2]Dr. K.K Paliwal, [3]Vikas Seth
[1]M.Tech, (CSE), PIET, Samalkha, Haryana, India
[2]Director, PIET, Samalkha, Haryana, India
[3]Professor, Department of CSE, PIET, Samalkha, Haryana, India

Abstract: ***Research on Mobile Ad Hoc Networks has been ongoing for decades. The history of ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program. Mobile Ad-hoc Networks are a collection of two or more devices equipped with wireless communications and networking capability. These devices can communication with other nodes that immediately within their radio range or one that is outside their radio range. For the later, the nodes should deploy an intermediate node to be the router to route the packet from the source toward the destination. The Wireless Ad-hoc Networks do not have gateway, every node can act as the gateway. This paper deals about the analysis of rural communication and its enhancement using mobile ad-hoc network.***

Keywords: MANET, Mobile communication, Radio Frequency, Rural network, RMUC.

I. INTRODUCTION

The challenge is to deliver a mobile service to rural users that can not only be viable, but be profitable at these low levels of Average Revenue Per User (ARPU). Currently, the mobile phone population in India is growing by eight million phones per month. But rural teledensity has yet to break the 5% barrier (despite television penetration levels of 26% and growing).

Improvement in communication technologies has made life easier. Rural sector is also benefitted with this advancement. The evolution of communication technologies has changed the way Rural fight the wars, the way they work and the way they exchange information. Despite of this advancement, Rural is also susceptible to same problems faced by other structured organizations; which is organizational communication. Communication is central to organizing and therefore is essential component to bring order out of chaos in organizational context.

Rural now requires high-speed broadband to be able to exploit the capabilities of smart phones. Traditional FM/AM based radio network with antenna or satellite transmission can no longer satisfy the need of information exchange in Rural when the network needs are instant. The major problem in achieving the efficient network technology is the dynamicity in network, bandwidth of deployed network, infrastructure requirement and security. The Rural requires the network which can be set up quickly in a temporary shelter or in areas affected by war, crisis or disasters. Cellular base stations and mesh networking, combined together, can give Rural the required speed, but these types of network requires setting up the base stations, configuring the devices, defining the protocols, which requires lots of time and is not suitable for instant network requirements.

Therefore, Rural requires a ubiquitous nature of network with very efficient routing mechanism and high degree of security to protect the Rural critical data and information. The network should be instantly deployable and must not require the infrastructure of any kind to be set up. This nature of anytime-anywhere network also must address the dynamicity of the topology inside Rural network and must be robust with least frequency of failure. Thus, Rural requires a ubiquitous nature of network with very efficient routing mechanism and high degree of security to protect the Rural critical data and information. This nature of anytime-anywhere network also must address the dynamicity of the topology inside Rural network and must be robust with least frequency of failure.

II. OVERVIEW OF RESULTS FROM RECENT STUDIES

- The Ant System: Optimization by a colony of cooperating agents way ant colonies function. [Marco Dorigo] [1996]. An analogy with the way ant colonies function has suggested the definition of a new computational paradigm, which we call ant system (AS). We propose it as a viable new approach to stochastic combinatorial optimization. The main characteristics of this model are positive feedback, distributed computation, and the use of a constructive greedy heuristic. Positive feedback accounts for rapid discovery of good solutions, distributed computation avoids premature convergence, and the greedy heuristic helps find acceptable solutions in the early stages of the search process. We apply the proposed methodology to the classical traveling salesman problem (TSP), and report simulation results. We also discuss parameter selection and the early setups of the model, and compare it with tabu search and simulated annealing using TSP. To demonstrate the robustness of the approach,

we show how the ant system (AS) can be applied to other optimization problems like the asymmetric traveling salesman, the quadratic assignment and the job-shop scheduling. Finally we discuss the salient characteristics-global data structure revision, distributed communication and probabilistic transitions of the AS.

- A survey on sensor networks [I. Akyildiz, W. Su][2002] This paper describes the concept of sensor networks which has been made viable by the convergence of micro-electro-mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored.
- Wireless Ad-hoc Networks [Lu Han] [2004] Mobile Ad-hoc Networks are a collection of two or more devices equipped with wireless communications and networking capability. These devices can communication with other nodes that immediately within their radio range or one that is outside their radio range. For the later, the nodes should deploy an intermediate node to be the router to route the packet from the source toward the destination. The Wireless Ad-hoc Networks do not have gateway, every node can act as the gateway. Mobile Ad-hoc Networks is a fundamental flawed architecture. The main reason for the argument is that Mobile Ad-hoc Networks are almost never used in practice, almost every wireless network nodes communicate to base-station and access points instead of co-operating to forward packets hop-by-hop. We take the position that Mobile Ad-hoc Networks (MANET) are a fundamentally flawed architecture. As argument, we try to clarify the definition, architecture and the characters of MANET, as well as the main challenges of constructing the MANET.
- Swarm intelligence for routing in mobile ad hoc networks [Gianni Di Caro][2005]Mobile Ad Hoc Networks are communication networks built up of a collection of mobile devices which can communicate through wireless connections. Routing is the task of directing data packets from a source node to a given destination. This task is particularly hard in Mobile Ad Hoc Networks: due to the mobility of the network elements and the lack of central control, routing algorithms should be robust and adaptive and work in a decentralized and self organizing way. In this paper, we describe an algorithm which draws inspiration from Swarm Intelligence to obtain these characteristics. More specifically, we borrow ideas from ant colonies and from the Ant Colony Optimization framework. In an extensive set of simulation tests, we compare our routing algorithm with a state-of-the-art algorithm, and show that it gets better performance over a wide range of different scenarios and for a number of different evaluation measures. In particular, we show that it scales better with the number of nodes in the network.
- Intrusion Detection in Mobile Adhoc Networks [Sevil Sen,John A. Clark] [2006]Intrusion detection on mobile ad hoc networks (MANETs) is difficult. This is because of their dynamic nature, the lack of central points, and their highly resource-constrained nodes. In this paper we explore the use of evolutionary computation techniques, particularly genetic programming and grammatical evolution, to evolve intrusion detection programs for such challenging environments. Cognizant of the particular importance of power efficiency we analyse the power consumption of evolved programs and employ a multi-objective evolutionary algorithm to discover optimal trade-offs between intrusion detection ability and power consumption.
- Mobile Ad hoc Networks: Challenges and Future [Kavita Taneja R. B. Patel][2007] An ad hoc network is a collection of wireless computers with dynamically changing topology, communicating among themselves over possibly multi-hop paths, without the help of any infrastructure. Although many ad hoc network routing protocols have been proposed (AODV, SAODV, DSR etc), none of them considers or solves the security problems efficiently within the restrictions of ad hoc networks. Ad hoc networks are vulnerable to many types of attack like Denial Of Service (DOS), Byzantine Attack, Black-hole Attack, Flooding Attack, etc. In this paper we put forward an efficient and reliable security mechanism based on the AODV routing protocol which protects the ad hoc networks from different types of flooding attacks.
- Security Issues in Mobile Ad hoc networks [Wenjia Li,Anupam Joshi][2012]In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.
- Key distributed cryptography using key algorithm in MANET [Rajesh kumar Dangi, Rachna Thakur][2013]Mobile Ad hoc Network (MANET for short) is a kind of communication network which is different from the traditional wireless network due to its characteristic of no central administration. It is a self-configurable and autonomous network, and consists of several independent nodes. MANET in recent years not only seen widespread use in domestic and commercial application areas but also becomes the focus of intensive research. Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking. In this paper, we study the security goals and solutions to be achieved and also use cryptographic schemes such as distributed cryptography, to build a highly available and secure key management service and also provide accurate routing information in a timely manner. The efficiency of a distributed cryptosystem strongly depends on the characteristics of the public key cryptosystem on which it is based. We propose an optimized encryption method which may be related with the RSA key generation and Diffie Hellman key exchange mechanism, to provide more security for data exchange. In this we perform splitting both,

plaintext before encryption and cipher text after encryption and also here we try to provide more security by combining both algorithms.

- Widely used ant colony optimization meta-heuristic was studied and some intelligent techniques like local transmission and automatic route discovery introducing the agents likeUANT. It was found that the concept of local transmission and automatic route discovery helps in reducing the overhead of system to great extent. The same concept is used to develop the prototype of UC application named RMUC.
- Artificially intelligent techniques were researched and it was used to model the new multi-agent based routing algorithm. The behavior of agents in network were studies and it was found that use of swarm intelligence helps in performing the collaborative tasks which cannot be performed by individual agents.
- The algorithm was compared with similar existing algorithms like ARA and AODV in terms of dynamicity, error handling and reducing overhead. It was found that the proposed routing algorithm proved to be better in reducing overheads and handling errors and was able to address the node mobility issues in MANET.
- A mobile ad hoc network is one of the most innovative and challenging areas of wireless networking and tends to become increasingly present in our daily life.
- There are various MANET protocols proposed by the subject to a variety of attacks through the modifications or fabrications of routing message or impersonations of other nodes.
- It allows the attackers to influence the victim's selection of routes or enable the denial of service attacks. Some major security issues in MANET were addressed by the researcher and measures to prevent such attacks were researched.
- The Parallel search algorithm protocol (PSO) provides excellent performance for routing in multi-hop wireless ad hoc networks.
- PSO has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, fast motion of all nodes in the network.
- A key reason for this good performance is the fact that PSO operates entirely on demand with no periodic activity of any kind required at any level within the network. As nodes begin to move more or as communication patterns change, the routing packet overhead of PSO automatically balance to only that needed to track the routes currently in use. This approach of intelligent routing is also used in collaboration with Ant Colony Optimization in the prototype built.

  All the research conducted was documented and the work of research was used to create a prototype. The concept of Ant colony optimization and PSO routing were used to create an efficient routing algorithm and security measures were provided in prototype using RSA encryption algorithm. The prototype is named RMUC and is designed for the efficient routing in Rural and Urban sector where the need of ubiquitous network is urgent.

III. OBJECTIVES OF RESEARCH

The prime reason for proposing the new model of network for Rural is majorly to introduce the ubiquity in the network. Anytime, anywhere available network is the need of Rural. The benefits of proposed network model are as follows:

1. Instant Setup

The proposed model of network uses Ad-hoc network for setting up the network. Therefore, the communication can be set up whenever required and can be terminated after it's over. This reduces the overhead in power consumption and routing because devices inside network are only active whenever required and communication can be set up and terminated anytime.

2. No Infrastructure requirements:

In SRMUC, every node is also a router. Hence, the job of routing is done by each and every node sharing the network load rather than by a single central routing device. Because of this reason, the network also is mobile because there is no requirement of setting up any central server for doing the routing or monitoring job. Network itself does the job of delivering the packets.

3. Self-Organizing:

All the nodes in RMUC are self-organized and are adaptive in nature. Any change in link due to node mobility is effectively handled. Therefore, it requires minimal human intervention which reduces the administrative cost.

4. Efficient Routing:

RMUC uses the best of PSO routing algorithm and Ant colony optimization which makes it an efficient network in terms of data delivery. PSO algorithm provides the intelligence to the nodes in determining the path and routes and the Ant colony optimization algorithm provides the optimal way to find the shortest path by emulating the real world ants.

5. High degree of security:

Proposed network model uses RSA to encrypt the critical information. So, the network becomes secured from the threats like eavesdropping, hacking of confidential information, and interference.

IV. PROBLEMS IDENTIFIED IN IMPLEMENTATION METHODOLOGIES

- **Load Balancing Routing in MANET**

Load Balanced Routing Various Load balanced ad hoc routing protocols are on-demand-based protocols; i.e load balancing strategies is combined with route discovery phase. In a broader context, the term load can be interpreted as:

Channel load: Represents the load on the channel where multiple nodes contend to access the shared media.
Nodal load: Relates to a node's activity. Specifically, it refers to how busy a node is in processing, computation, and so on. Neighboring load: Represents the load generated by communication activities among neighboring nodes. Load metrics Load balanced ad-hoc routing protocols are based on different load metrics.

- **Active path:** This refers to the number of active routing paths supported by a node. Generally, the higher the number of active routing paths, the busier the node since it is responsible for forwarding data packets from an upstream node to a downstream node.
- **Traffic size:** This refers to the traffic load present at a node and its associated neighbors (measured in bytes).
- **Packets in interface queue:** This refers to the total number of packets buffered at both the incoming and outgoing wireless interfaces.
- **Channel access probability:** This refers to the likelihood of successful access to the wireless media. It is also related to the degree of channel contention with neighboring nodes.
- **Node delay:** This refers to the delays incurred for packet queuing, processing, and successful transmission.

V. THE CHALLENGES OF MOBILE COMMUNICATION RURAL INDIA

There are four main difficulties in serving rural communities, each one of which has appeared insurmountable:

- Power challenges – Most of rural India is not served by the power grid. Some areas may get 'agricultural power' – two hours in the morning and evening – but even this is the exception. When fuel can be afforded and delivered, power tends to come from diesel generators. The combination of poor fuel quality and poor generator maintenance severely limits the life of any generator.
- Revenue challenges – Rural India can pay for mobile services, but only around $2 per month. The cost base of any solution has to be geared to these ARPU levels.
- Skills challenges – There are no trained telecom engineers and few people can read or write. This makes the installation and maintenance of GSM networks highly challenging.
- Access challenges – These are extremely remote communities, served by poor roads and no other significant infrastructure.

VI. PROBLEM DEFINITION

The existing infrastructure based Rural network works on antenna and satellites. Communication devices are linked to central routing device and the communication takes place in the form, source device-central router-destination device. Each and every piece of information inside the network is processed and routed by the central routing device. This approach of communication has some drawbacks, which are:

1. Requires infrastructure:

It requires setting up the antennas or launching the satellite which will act as central server for all the communications taking place inside network.

2. Time consuming set-up process:

Setting up the devices, configuring the nodes etc. is time consuming job. Therefore, the set-up of the network requires huge investment of time in first installment.

3. Susceptible to interference:

Since, the devices need to communicate with central router; every time they want to communicate the data on the link may be susceptible to interference by intruder. The communication links become more obvious to intruders in this kind of network, jeopardizing the whole network.

VII. IDENTIFICATION IN SECURITY METHODOLOGIES

Now a day, it is no longer optional to have security solutions even inevitable for every kind of organizations and individuals. There are number of generic tools which are common for organizations as well as for individual users to provide security which includes; Anti-Spam, Anti-Virus etc., and network security have become essential issue in MANET. Security is one of the main issues in the MANET especially with respect to size and complexity of the network. The aim of the thesis is to discuss different aspects of security in MANET (e.g. multi-layer intrusion detection technique in multi hop network of MANET, security problems relates between multihop network and mobile nodes in MANET etc) and also implement some of the solutions (e.g. comparative study of different routing protocol (AODV, DSR and TORA) security threats within MANET network like intruder behavior, tapping and integrity, MANET link layer and network layer operations with respect to information security etc) with respect to MANET network.

This report also discusses different number of scenarios of MANET network which we implement in our simulation. In our simulation we use to implement different routing protocols and also did comparative study that which one is better with respect to different aspects. We also use to implements mechanisms of intruder behavior, tapping and integrity, and MANET link layer and network layer operations with respect to information security.

VIII. SECURITY IN AD HOC NETWORKING PROPOSALS

1.7.1 DDM

Dynamic Destination Multicast protocol (DDM) is a multicast protocol that is relatively different from many other multicast-based ad hoc protocols. In DDM the group membership is not restricted in a distributed manner, as only the

sender of the data is given the authority to control to which the information is really delivered. In this way the DDM nodes are aware of the membership of groups of nodes by inspecting the protocol headers.

The DDM approach also prevents outsider nodes from joining the groups arbitrarily. This is not supported in many other protocols directly; if the group membership and the distribution of source data have to be restricted, external means such as the distribution of keys have to be applied.

1.7.2 OLSR

Optimized Link State Routing protocol (OLSR), as defined in , is a proactive and table driven protocol that applies a multi-tiered approach with multi-point relays (MPR). MPRs allow the network to apply scoped flooding, instead of full node-to-node flooding, with which the amount of exchanged control data can substantially be minimized. This is achieved by propagating the link state information about only the chosen MPR nodes. Since the MPR approach is most suitable for large and dense ad hoc networks, in which the traffic is random and sporadic, also the OLSR protocol as such works best in these kinds of environments. The MPRs are chosen so that only nodes with one-hop symmetric (bi-directional) link to another node can provide the services.

1.7.3 ODMRP

On-Demand Multicast Routing Protocol (ODMRP) is a mesh-based multicast routing protocol for ad hoc networks, specified in. It applies the scoped flooding approach, in which a subset of nodes - a forwarding group - may forward packets. The membership in the forwarding groups are built and maintained dynamically on-demand. The protocol does not apply source routing. ODMRP is best suited for MANETs where the topology of the network changes rapidly and resources are constrained. ODMRP assumes bi-directional links, which somewhat restricts the potential area of application for this proposal; ODMRP may not be suitable for use in dynamic networks in which nodes may move rapidly and unpredictably and have varying radio transmission power. Currently ODMRP does not define or apply any security means as such, "the work is in progress". The forwarding group membership is controlled with the protocol itself, though.

1.7.4 AODV and MAODV

Ad Hoc On-Demand Distance-Vector routing protocol (AODV), defined in [11], is an unicast-based reactive routing protocol for mobile nodes in ad hoc networks. It enables multi-hop routing and the nodes in the network maintain the topology dynamically only when there is traffic. Currently AODV does not define any security mechanisms whatsoever.

The authors identify the necessity of having proper confidentiality and authentication services within the routing, but suggest no solutions for them. The IPSec is, however, mentioned as one possible solution. Multicast Ad Hoc on-Demand Distance-Vector routing protocol (MAODV), specified in [12], and extends the AODV protocol with multicast features. The security aspects currently noted in the design of MAODV are similar to the AODV protocol.

IX. REASON FOR PROPOSING THIS TECHNIQUE

This is a new approach to delivering profitable mobile services to rural India and beyond. It's the first example of micro telecom, the re-engineering of telecommunications to meet the needs of rural and remote communities. This is a complement to existing GSM networks, extending them to seize the rural opportunity. It is:

Low-power – at less than 50W per Base Station, the entire system can be run on solar power. No power grid or generator necessary.

Low cost – a fraction of the cost of traditional GSM Base Stations; profitable at very low densities and ARPUs.

Fully GSM standards compliant – easily links to existing networks, dramatically extending their reach.

Self-contained – With BSC and MSC functionality integrated and deployed in the field on Base

Near-Zero Maintenance – update software remotely and perform simple swap repairs if needed.

Cascading Star Architecture – a unique, modular architecture optimized for low-cost rural Expansion; with local switching to minimize backhaul.

X. CONCLUSION

Researcher has worked on the routing algorithm based on swarm intelligence called Ant Colony Metaheuristics and derived a customized algorithm for routing in dynamic nature of wireless network. The algorithm addressed the popular issues in Mobile Ad-Hoc Networks like, node mobility, automatic route management and load balancing. The algorithm is also used to design the prototype for military mobile network named RMUC. Despite of all the research and findings in the researcher's work there are still some issues which are not addressed by the work of the researcher and require some new learning to overcome. Following section describes the assumptions made, issues faced and new learning required to address those issues in future.

REFERENCES

[1] Zhou, L. and Haas, Z. Securing Ad Hoc Networks. 1999.

[2] Ji, L. and Corson, M. S. Differential Destination Multicast Specification (DDM). IETF draft, 12 July 2000.

[3] Jacquet, P. et al. Optimized Link State Routing Protocol (OLSR). IETF draft, 18 July 2000.

[4] Perkins, C. and Royer, E. Multicast Ad Hoc On-Demand Distance-Vector Routing (MAODV). IETF draft, 11 July 2000.

[5] Perkins, C. et al. Ad Hoc On-Demand Distance-Vector Routing (AODV). IETF Draft, 14 July 2000. [referred 25.9.2000]

[6] Miller, L., & Pallot, X. (2001). *Mechanisms for implementing priority* at the 802.11 MAC layer. Implementation of Priority Schemes in MANETs over the 802.11 MAC layer, 11-13.

[7] Erl, T. (2004). *"Service-oriented architecture".* Englewood Cliffs: Prentice Hall.

[8] Erl, T. (2005) *"Service-oriented architecture: concepts, technology, and design".*

[9] S, M. G., & Sharma, S. C. (2010). Manet Envorinment Variations. Analyzing The Manet Variations, Challenges, Capacity And Protocol Issues, 15.

[10] Bhadani, A., & Chaudhary, S. (2010, January). *"Performance evaluation of web servers using central load balancing policy over virtual machines on cloud".* In Proceedings of the Third Annual ACM Bangalore Conference (p. 16). ACM.

[11] Chen, T. L., Hsu, C. H., & Chen, S. C. (2010). "*Scheduling of job combination and dispatching strategy for grid and cloud system".* In Advances in Grid and Pervasive Computing (pp. 612-621). Springer Berlin Heidelberg.

[12] Babar, M. A., & Chauhan, M. A. (2011, May). "*A tale of migration to cloud computing for sharing experiences and observations*". In Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing (pp. 50-56). ACM.

[13] Oracle Corporation. (2012). *Listing Network Interface Address*. Retrieved October 4, 2013, from The Java Tutorials: http://docs.oracle.com /javase/tutorial /networking/ nifs/listing.html

[14] How2Pass Network. (2012). *Router Basics. Retrieved October 3, 2013,* from How2Pass: http://www.how2pass.com/CCNA/study_material/routerbasics.htm

[15] Electronic manufacturers. (2007). "*Wireless Router. Retrieved October 3, 2013,* from Electronic Manufacturers Web Site: http://www.electronics-manufacturers.com /products/computer-networking/wireless-router/

[16] Survey ofLoad Balancing Routing in MANET , Mrs.ASHWINI.B.PATIL, Volume 1, Issue 3, September – October 2012, ISSN 2278-6856 (ijettcs)

[17] Chai Keong Toh , Anh-Ngoc Le and You-Ze Cho "Load Balanced Routing Protocols for Ad Hoc Mobile Wireless Networks" IEEE CommunicationsMagazine • August 2009

