RESEARCH ARTICLE

A Study on Requirement and Issues in Mobile Speed Network

Bhupender: bhupy_28@yahoo.in
Student, M.Tech
Department of Computer Sc. & App., MDU,
Rohtak, Haryana

Gopal Singh: gsbhoria@gmail.com
Assistant Professor,
Department of Computer Sc. & App., MDU,
Rohtak, Haryana

Abstract: Mobility is the core property of mobile network. But such network can have fixed or mobile communicating nodes. A special categorization of mobile network in which communicating nodes are moving in high speed is called speed network. In such network, algorithmic approach and the network throughput depends on node speed and dynamic architecture. In this paper, a detail study on speed network is provided along with associated issues. The paper has discussed in hidden challenges associated with speed network.

Keywords: Speed Network, Direction Analysis, Speed Analysis, Handoff

I. INTRODUCTION

A Mobile network is one of the most available decentralized system in which nodes are generally in moving position. Because of these moving capabilities, the nodes enter and exit from one network to other. When a new node enters to some network, it cannot be treated as the suspicious node because of open nature of the network. This dynamic nature of mobile network is itself a challenge in terms of mobility in the network. Each node in mobile network itself acts as a host or the router. To perform the communication with any node, each node depends only on his current neighbors and these neighbor nodes are not fixed. It means the communication in mobile network cannot be fully reliable at any time.

Mobility in such network is always the major concern in mobile network. It gives the problems associated to the mobile network such as handoff mechanism. It is defined under different vectors of confidentiality, reliability, integrity of the data as well as nodes. There are number of issues faced by a mobile network because of different mobility, shown in figure 1. The open medium here defines the different kind of communication medium available for communication at the same time and during communication it can switch to these communication medium because of open nature. The dynamic topology formation defines the inclusion and exclusion of any node dynamically to the network so that the issues because of mobility get increased.
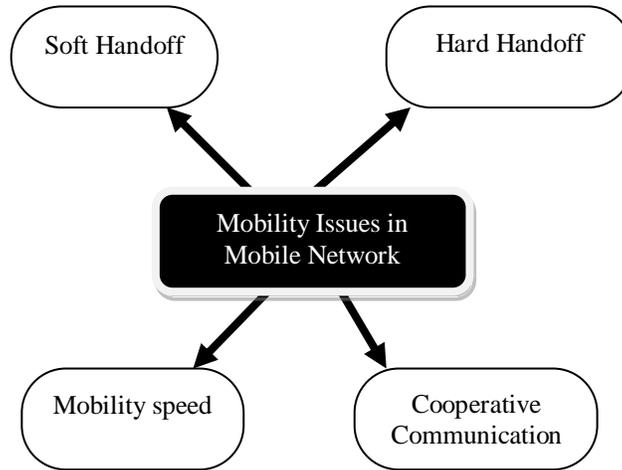
Figure 1 : Mobility Based Issues MANET

The decentralized system here means there the lack on central control or the management to the mobile network. Each node itself behaves independently without the control of any central entity. Each node itself behaves as the node as well as the router. The cooperative communication in network is difficult because of mobile nature. No node is considered as the term neighbor so that the neighbor node search required while initializing the communication each time. In this communication network. Another issue with mobility is the speed. Higher the speed, lesser the coordination or tracking of node for communication. High speed gives higher chances of data loss and data fading. To provide the effective network communication, low speed node movement gives more reliable communication over the network.

Another issue associated with mobile network is the handoff mechanism. Handoff mechanism is one of the most crucial communication terms that gives the switching between the clusters. Each mobile node is controlled by some base station and each base station is defined with specific range. As a node moves outside its current coverage range, then it is required to identify the next controller to that that that will get the node access. This mechanism of transferring the control is called handoff mechanism. Handoff mechanism can be hard handoff or soft handoff. Soft Handoff is performed between two similar networks whereas hard handoff is done between two different network types. In a hybrid communication network hard handoff is more challenging communication activity that occurs because of speed networks.

In this paper, a study on mobile networks along with relative properties and issues. The paper has discussed the speed network in which the requirements and consequences of node mobility is analyzed. In this section, an introduction to speed network along with relative issues is given. In section II, the work defined by earlier researchers is given. In section III, the challenges in speed network is defined. In section IV, the conclusion obtained from the work is presented.

II.   EXISTING WORK

As the network security is one of the most critical issues for mobile networks, because of this, lot of concern is given to the security threats in mobile networks. Some of the work defined by earlier researchers is discussed in this section. In year 2010, Axel Kring has presented a neighborhood monitoring mechanism for adhoc network. Author presented a k-hop analysis based mechanism under defined constraints so that the network limitations will be handled. Author has defined the work on the malicious node detection by performing the dynamic analysis on neighboring nodes [1]. Another work on the malicious node detection was proposed by Ying Li in year 2011. Author defined the work on tracking based scenario. Author defined the mathematical and probabilistic framework for the detection of attacks and the exceptions [2]. Another work on the malicious node detection and a secure routing was presented by Bogdan Carbunar in year 2004. Author investigates the security threats in mobile networks so that the reliable communication will be drawn from the communication. Author has defined a secure infrastructure oriented communication in misbehaving mobile networks [3].

101

A work on the exploration of hijacking attack and the preventive mechanism was presented by Johann Schlamp in year 2012. Author has defined a security based work to identify the spam packets during the communication process as well as provided an effective approach to detect the victim. Author has defined the analysis through the IP prefix analysis so that the long term benefits will be obtained from the work. Author has defined the incidental communication and control mechanism in mobile network [4]. A control mechanism to restrict the outgoing spam communication was handled by Joshum Goodman in year 2004. Author has defined the conventional technique to analyze the message packets under different techniques so that the life time of the network communication will be increased. Author has defined the work to obtain the maximum profit from the communication so that reliable communication effect will be drawn[5]. Danny Dhillon has defined the work to improve the communication integrity in case of intrusion mobile network. Author defined the safeguard based approach to increase the detection rate so that effective communication schedule will be obtained [6].

Ahmed Khurshid has presented a work on the real time analysis on different network invariants that affects the network flow. Author presented a controller device based approach to control the forwarding communication as well as the reliable communication will be drawn from the network[7]. Another work on the blackhole detection was presented by Evan Cooke in year 2004. Author defined the exploration of work under the traffic analysis so that reliable packet communication will be performed. Author defined the work based on Internet Motion sensor so that the infrastructure based effective communication will be drawn from the network[8]. A work on the effective routing in opportunistic network was presented by Umair Sadiq in year 2012. Author presented the forwarding rate analysis along with packet loss analysis to identify the communication incentive. Author presented the work to analyze the control in non linear communication network. Author defined the work in the optimal conditions so that the flow maximization will be performed[9]. The exploration of the node replication attack was presented by Mauro Conti. Author presented a energy and memory effective solution in a constrained network so that reliable communication path will be obtained[10]..

Garima Gupta has defined a work on blackhole attack and provides a delay effective scheme to minimize the attack hazards. Author defined the characteristic analysis based algorithm generate an effective route under the malicious node attack. Author defined the probabilistic behaviors analysis scheme to provide the solution against the blackhole attack[11]. A work on the topology aware analysis approach to reveal the security scheme in mobile networks. Author presented an isolated mechanism to handle the attacks and to reduce the false detection rate. Author presented a overhead analysis approach to improve the network reliability and to minimize the attack impact in mobile network[12]. A two dimensional analysis approach to improve the network QoS under different adversarial environments was presented by Peter J.J. McNeney. Author discussed two main issues to improve the QoS and to improve the network reliability. Author defined a single path adaptation and multipath adaptation mechanism to improve the network bandwidth and to incrase the network reliability[13].

III.   CHALLENGES IN SPEED NETWORK

In this section, different vectors or the challenges associated with route identification is been discussed. A speed network is defined with lesser centralized control and lesser capabilities. Because of these restrictions, the routing in such network is always a challenge. The factors that affect the route generation and identification are shown in figure 2.

A)   Node Deployment

The node localization in a speed network defines the physical parameter that affects the network performance. The deployment can be either randomized or the deterministic. In case of deterministic placement, the nodes are placed at specific locations under some defined architecture. The distribution of nodes under some specific order also improves the network uniformity and the clustering so that the energy efficient processing will be performed over the network. The effective localization is defined under different vectors such as sensing range, bandwidth, type of network architecture etc.
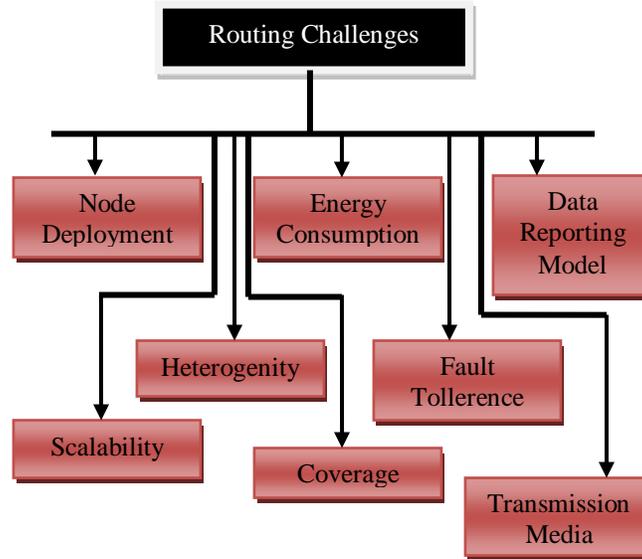
102

Figure 2 : Challenges Associated with Routing

B)   Energy Consumption

Each node in speed network is defined with limited energy. When some communication or the computation is performed over the network, each participating node loses some amount of energy. Because of this, the routing decision is performed under the energy awareness. It is required to generate a fault free communication, because re-routing or the reconstruction of network gives heavy energy loss. Another problem of network is the energy balancing. It means, the communication should be performed in such way, the energy consumption over the network will be performed in symmetric way otherwise, the unequal energy distribution over the network reduces the energy consumption and increases the criticality of energy challenges

C)   Data Reporting Model

The data reporting or the sensing is about to deliver the information periodically to the base station. This data reporting model can be either event based, query based, time based or hybrid. The data diffusion approach is applied along with data reporting model to represent the type of information collection and the distribution. This kind of model also performs the monitoring to the network nodes and identifies the sudden changes so that more accurate and reliable communication will be performed.

D)   Heterogeneity

When the network is constructed over the homogeneous nodes, the node replacement can be done easily. But when the capabilities of each node are defined, the criticality over the network is increased. In such case, a node cannot replace other node. The degree of heterogeneity affects the network capabilities. The special sensors are defined to perform specific operations so that the service oriented constraints are specified while performing the routing decision. The route identification becomes more specific in such network, so that the route optimization is required to perform under certain limits.

E)   Fault Tolerance

In speed network, a node can fail or block because of different reasons. The reason can be potential damage, some attack, lack of power or some environmental interference. While performing the route selection, the fault free participating nodes are selected so that the reliable communication will be performed. Some agents or the monitor nodes are placed over the network to identify the faulty nodes or links so that fault tolerance communication will be performed over the network.

F)   Scalability

As the size of the network, the criticality of network communication and route identification also increases. The distance communication is performed using multi-hop routing and in such case, the identification of route with minimum number of intermediate nodes is also a challenge. As the number of intermediate nodes increases, the energy consumption over the route also increases. The scalability also need to identify the node state so that effective utilization of each node over the network will be performed.

G)   Coverage

Coverage is defined as the sensing range that decides the communication reach of a node. Higher the range, more accurate the communication will be. The coverage is also limited to the physical area of the network. The sensing node also identifies the maximum connectivity over the network. Higher the connectivity level, more effective the routing decision will be.

H)   Transmission Media

A speed network performs the communication over the wireless channel under different vectors associated with communication channel. Some such vectors includes fading rate, error rate etc. Communication bandwidth, communication rate, MAC protocol design are also the integrated vectors with transmission media that affects the efficiency and reliability of communication over the speed network.

IV.   CONCLUSION

A Mobile network is open area network with dynamic network architecture. But the criticality of network increases with the specification of speed architecture. In this paper, an introduction to speed network is given. The paper has discussed the characteristics and associated challenges.

REFERENCES

[1]   Axel Krings," Neighborhood Monitoring in Ad Hoc Networks", CSIIRW '10, April 21-23, 2010, Oak Ridge, Tennessee, USA ACM 978-1-4503-0017-9

[2]   Ying Li," Component-Based Track Inspection Using Machine-Vision Technology", ICMR'11, April 17-20, 2011, Trento, Italy ACM 978-1-4503-0336-1/11/04

[3]   Bogdan Carbunar," JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks", WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA. ACM 1-58113-925-X/04/0010

[4]   Johann Schlamp," How to Prevent AS Hijacking Attacks", CoNEXT Student'12, December 10, 2012, Nice, France. ACM 978-1-4503-1779-5/12/12

[5]   Joshua Goodman," Stopping Outgoing Spam", EC'04, May 17–20, 2004, New York, New York, USA. ACM 1-58113-711-0/04/0005

[6]   Danny Dhillon," Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada. ACM 1-59593-306-9/06/0007

[7]   Ahmed Khurshid," VeriFlow: Verifying Network-Wide Invariants in Real Time", HotSDN'12, August 13, 2012, Helsinki, Finland. ACM 978-1-4503-1477-0/12/08

[8]   Evan Cooke," Toward Understanding Distributed Blackhole Placement", WORM'04, October 29, 2004, Washington, DC, USA. ACM 1-58113-970-5/04/0010

[9]   Umair Sadiq," CRISP: Collusion–Resistant Incentive–Compatible Routing and Forwarding in Opportunistic Networks", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10

[10]   Mauro Conti," A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Speed networks", MobiHoc'07, September 9-14, 2007, Montréal, Québec, Canada. ACM 978-1-59593-684-4/07/0009

[11]   Garima Gupta," Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks", Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10

[12]   Abhijit Das," Energy Aware Topology Security Scheme for Mobile Ad Hoc Network", ICCCS'11, February 12–14, 2011, Rourkela, Odisha, India. ACM 978-1-4503-0464-1/11/02

[13]   Peter J. J. McNerney," A 2-Dimensional Approach to QoS Provisioning in Adversarial Mobile Ad Hoc Network Environments", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10