J. Software Engineering & Applications, 2009, 2:50-54
Published Online April 2009 in SciRes (www.SciRP.org/journal/jsea)

Research on Survivability of Mobile Ad-hoc Network

Yuan Zhou[1], Chunhe Xia[1], Haiquan Wang[1], Jianzhong Qi[1]

[1]Key Laboratory of Beijing Network Technology, School of Computer Science and Engineering, Beihang University, Beijing, China. Email: zhouyuan84825@163.com

Received November 26th, 2008; revised January 7th, 2009; accepted February 16th, 2009.

ABSTRACT

In this paper, we analyze the survivability of Mobile Ad Hoc Network systemically and give a detailed description of the survivability issues related to the MANET. We begin our work with analyzing the requirements of survivability of ad hoc network, and then we classify the impacts that affect survivability into three categories: dynamic topology, faults and attacks. The impacts of these factors are analyzed individually. A simulation environment for the MANET towards survivability is designed and implemented as well. Experiments that under the requirements and the impacts we declared are done based on this environment.

***Keywords*:** *Ad hoc*, *Survivability*, *GTNeTS, Simulation*

1. Introduction

A mobile ad-hoc network (MANET) is a kind of self-organized wireless network with a collection of mobile hosts that is multi-hop instead of using any fixed infrastructure or centralized management [1,2,3]. There are a lot of potential applications of MANET in both civilian and military areas. For instance, it can be applied in disaster communications, used as the back-up network of traditional mobile communication networks and used to build tactical network, etc. With the characteristic of MANET like: dynamic topology, no infrastructure or trust institution and limited power resources, research on survivability of MANET is becoming an academic hotspot.

The concept of survivability was first presented by Barnes in 1993. After that, Knight, K.Sullivan, R. J. Ellison and many research institutes have done lots of effort on issues of survivability. To be brief, survivability is the capability of a system to provide essential services under attacks, failures or accidents. At present, many researches of MANET survivability put emphasis on designing new survivable routing protocols for specific problems [4,5]. However, there is few integrated and systematic analysis in the MANET survivability area [6]. On the other hand, research institutions usually use simulation approaches for experimental verification on MANET. However, the existing MANET simulators are mainly constructed for the purpose of experimenting performance or protocol of MANET [7]. Attributions related to MANET survivability are absent in the simulator structure. Additionally, threats like faults and attacks can not to be brought in to those simulators easily to verify MANET survivability issues.

For the above reasons, this paper presents a systematic analysis of MANET towards survivability. It describes how various impacts affect the survivability of MANET in details. Meanwhile, a simulation environment is designed and implemented for MANET towards survivability, which incorporates not only the attributions related to MANET survivability but also fault events and attack events against MANET. Users can draw many kinds of scenarios of MANET to test survivability issues under this simulation environment.

2. Analysis of Survivability of MANET

2.1 Definition of Survivability

Barnes presented the conception of "Survivability" for the first time in 1993, but until now, there is no all-acceptant definition of Survivability. The most influencing definition is presented by a research group of CMU/SEI, who define survivability as the capability of a system to fulfill its mission in a timely manner, in the presence of attacks, failures, or accidents [8]. Many other researchers define survivability from different perspective: In the area of software engineering, Deutsch defined surviva- bility as the degree to which essential functions are still available even though some part of the system is down [9]. Ellison *et al*. introduced the following definition: survivability is the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner [10]. Researchers like Moitra [11], Jha [12], and Wilson [13] also defined the survivability similarly.

This work was supported by three projects: the National 863 Project -Research on high level description of network survivability model and its validation simulation platform under Grant No.2007AA01Z407, The Co-Funding Project of Beijing Municipal education Commission under Grant No.JD100060630 and National Foundation Research Project.

The definitions above well describe the meaning of survivability in natural language, but attributions towards survivability are not embodied, especially those of the MANET. Compared with the descriptive definition, a formal description can give a more rigorous definition of survivability of MANET.

2.2 Definition of Survivability of MANET

After analyzing the definitions listed above, we find that the essence of survivability is the ability of providing essential system-wide service. Papers [6,14,15] presented that the essential service a mobile ad hoc network must provide is the communication service. That is to say, in the context of MANET, the essential service is primarily pivotal to a fundamental requirement: establishing a connection between any two nodes in an ad hoc network at any instant. So the survivability issue depends on how well an ad hoc network demands the requirement. On the other hand, the threads mobile ad hoc network must face to are as follows:

1) Dynamic topology influence. Nodes in an MANET can move arbitrarily. Consequently, network topology may change rapidly and randomly.

2) Faults that may happen in nodes and links. For instance, a node can shutdown itself for certain reasons, and a link may be influenced by an obstacle.

3) Every layer of ad hoc network architecture may be under attack. The Wormhole, Blackhole attacks aim at the network layer, jamming and eavesdropping attacks aim at the physical layer, and SYN flooding attacks aims at the transport layer, to name a few.

With the above analysis we can define the survivability of a mobile ad hoc network as, the ability of establishing a communication service between any two nodes in the network at any instant under the impact of dynamic topology, faults and attacks.

2.3 Detailed Description of Survivability of MANET

Based on the definition of survivability of MANET above, the system of MANET towards survivability issues can be abstracted into three members: mobile ad hoc network, the impacts which can affect the survivability of the mobile ad hoc network, and the essential service that a mobile ad hoc network must provide. It can be described as follows. Then, we will analyze them in detail

$$SurvivalAdhoc=\{ADHOC,SERVICE,IMPACT\} \quad (1)$$

The mobile ad hoc network is composed of a number of nodes with certain attributions related to the survivability and directed links. We consider the node obtaining following attributions: IP address, location, radio range, state (transmit, receive, idle and down), power, protocol type and, mobility type. All these attributions are related to the survivability of MANET. It can also be described as follows:

$$ADHOC::=\{NODE,LINK\} \quad (2)$$

$$NODE::=\{node_1,node_2,\ldots node_n\} \quad (3)$$

$$LINK::=\{<node_i,node_j>|node_i,node_j \in NODE\} \quad (4)$$

$$node=(ip,id,location,R,state,power,\ protocoltype,mobilitytype) \quad (5)$$

The essential service of a mobile ad hoc network is to establish a communication service between any two nodes in the network at any instant. The ad hoc network establishes a connection by two steps. First, connections between any two adjacent nodes are provided by the link layer and physical layer, and then such connections are extended by the network layer form one-hop to multi-hops. That is to say: for an ad hoc network with N nodes, there need to be a directional path ($Node_i$, $Node_j$…$Node_l$, Nod_m,) between any two nodes. And the path must meet the following requirements:

1) The distance between any two nodes in neighbors, $Node_i$ and $Node_{i+1}$, is less than the transmission range of $Node_i$.

2) Any node in this path must possess a routing entry that sets the target node as the destination node, and the next hop is the succeeding node.

The impacts affecting the ad hoc network survivability are dynamic topology, faults and attacks. The essence of all these three factors is to destroy the path between two nodes so that the network is disconnected. Thus, the factors are described as follows:

$$IMPACT ::= \{a \mid DynamicToplogy(a) \vee Fault(a) \vee Attack(a), a \in Actions\} \quad (6)$$

The factor of dynamic topology is caused by the actions such as mobility of nodes. It can result in the location changed of the node, and lead to the distance requirement of link layer connection dissatisfied. The influence of dynamic topology is that the new distance of two nods in neighbor may be larger than the transmission range of the first node, so that the path is destroyed. If there is no other path between the destination node and target node, they can't afford the communication service.

Faults are considered to include node faults and link faults [14]. Node faults are the actions that cause the state of the nodes changed to down. If the state of a node is changed to down, the transmission range will be changed to 0, which will make the path dissatisfy the requirement. Link faults are introduced by obstacles between nodes, or by signals fading effect which may influence the transmission range of nodes. It can be described as follows:

$$Fault(a) \rightarrow Node(a) \vee Link(a), a \in Actions \quad (7)$$

Attacks of MANET are usually classified by network layers. The attack aiming at the application layer is more or less the same as the wired network. Its main object is to disrupt the application service, and worm is an instance. Attacks to the transportation layer are the actions to disrupt the transportation layer protocols, like SYN flooding. The attacks to the network layer are the actions that destroy the routing and forwarding processes in ad hoc network [16]. The attacks to link layer are the actions

which destroy the connection of adjacent nodes. The attacks to physical layer are actions to jam, intercept or to eavesdrop the wireless channel. The description of attacks to network survivability is:

$$Attack(a) \rightarrow PhysicalAttack(a) \vee LinkAttack(a) \vee NetworkAttack(a) \vee TranspAttack(a) \vee ApplicationAttack(a) \quad (8)$$

3. Simulation Environment

Existing simulators are not well-equipped to serve our purpose. Hence, we design a survivability-based simulation environment of MANET to test how those factors influence the network.

3.1 Characteristics of Simulation Environment

While designing the simulation environment, we concern the following factors:

• Towards Survivability: The users can configure the parameters freely, such as node amount, mobility model, radio range, and power of node, which may affect MANET survivability. Fault events and attack events can be added to simulate scenarios towards survivability thoroughly.

• Expandability: Users can easily expand the simulation environment by adding new protocols of various layers, modules, attack events and fault events. For this reason, MANET towards survivability description language is designed and a language translator is implemented for it. Users can add new protocols, functions, faults and attacks through appending new keywords.

• Introduce Fault-event and Attack-event: Based on the definition and description of MANET survivability, faults and attacks are described, modeled and simulated to support MANET survivability verification.

• Data Acquisition Interface: One of the most important purposes of simulation is collecting data for further analysis from simulation process. Thus, data acquisition interface is incorporated in the simulation environment and users are allowed to configure what kind of result to be collected.

Based on the analysis above, simulation environment includes description language of MANET towards survivability and its interpreter. Then, we choose Georgia Tech Network Simulator (GTNetS) [17] as the underlying network simulation platform.

3.2 Simulation Environment Architecture

The system architecture is as shown in Figure 1:

•Graphic Configuration Interface: MANET properties, attack-events and fault-events information are configured by users through graphic user interface (GUI) and then be saved in the configuration file.

• Event interpretation: it analyzes and interpreters the configuration file, executes corresponding events by calling functions from event class library. The event class library consists of fault class library and attack class library, each of which is built up by specific classes. Currently, there are node fault classes, link fault classes in fault class library. And the attack class library contains energy-consuming attack class, signal interference attack class, black hole attack class, SYNflooding attack class and Worn attack class. All these classes are used by receiving parameters from the interpreter and calling support functions from GTNetS.

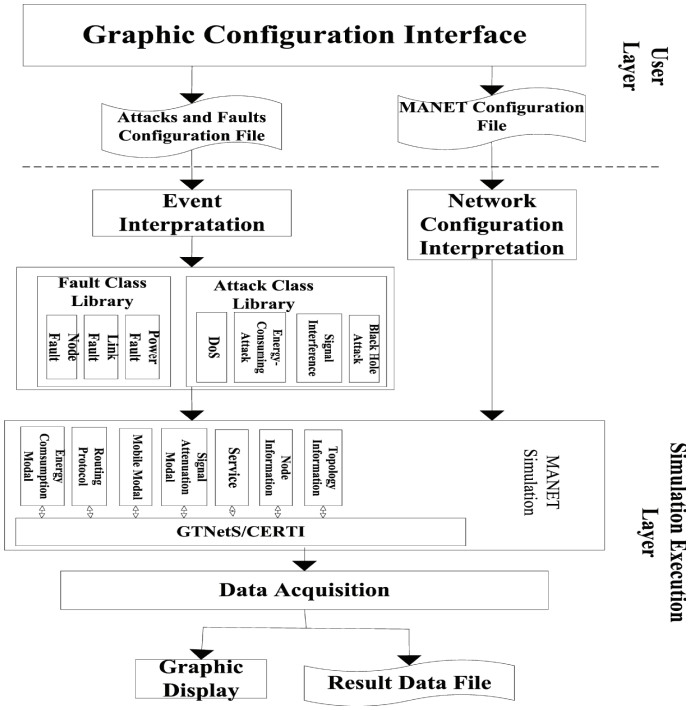

Figure 1. Simulation environment architecture

• Network configuration interpretation: it interprets the network configure file and makes function calls from GTNetS to construct simulation of MANET. All these network properties are supported: energy-consumption modal, AODV and DSR routing protocol, Random Waypoint, Random Walk and Random Direction mobility models, data transfer service, node information and topology information.

• Data Collection Module: it displays the simulation process graphically. After that, it parses the collected data that users care about, including total data transferred amount, average connectivity node-pairs and so on, then saves data into the result data file.

4. Experiments on MANET Survivability Analysis

4.1 Related Definition

For the simulation test of the definition of MANET survivability, the capability to provide connectivity service under various threats, terms that used in this paper are as follows:

Average Connectivity Efficiency [6] (E): It means the ratio of connected node pairs to all the node pairs within an N-node MANET in a certain period. In such MANET, each link between two nodes is directed, which means node *pair* (i,j) is different from node *pair* (j,i). The value of (E) reflects the capability of a MANET to provide connectivity service at a certain time. It reaches 100% when all the node pairs in the network can be connected.

$$Average\ Connectivity\ Efficiency(\%) = \frac{\sum_{i=1}^{T} (no.of\ \ connected\ \ node\ \ pairs)*100}{T*Number\ \ Of\ \ Node-pairs} \tag{9}$$

4.2 Experiment of Influences of Dynamic Topology

We choose number of node, radio range of node and mobility speed of node as the variables in this experiment. We would like to figure out that how the dynamic topology influences the survivability of MANET.

We carry out the experiment in a 1000×1000 bounded squared topology, and Parameters used in the test of the influences on MANET survivability of dynamic topology are as follows:

- Simulation time:300
- Node amount:20-80
- Radio range of each node:50-250
- Mobile way of node: Random Walk, 10-20
- Routing protocol of each node :AODV
- Bandwidth of each link:1Mb

From the results we can easily find out that when the radio range increases, the connectivity efficiency increases. Howeverm, its effect to the connectivity efficiency is not obvious when the radio range invreases to a certain level.As a result, when choosing the radio range, we should consider its effort to the connectivity efficiency and its cost to the power consumption.

When the moving speed of node increases, the topology is more instable, which means the node will be easier to move out of other nodes' transmission range, so that the connectivity efficiency decreases.

A larger number of nodes mean a higher node density. So from the results we can see in a bounded area, large number of nodes will contribute to the connectivity efficiency.

4.3 Experiment of Influence of Faults and Attacks

There are node faults and link faults. When node faults happen, nodes can shut down themselves randomly. When link faults happen, it can be emerging obstacles that affect the links. This paper assumes that only one fault happens at one time, and ignores the mobility attribution of the nodes, so that the topology is stable when dealing with the influences of faults.

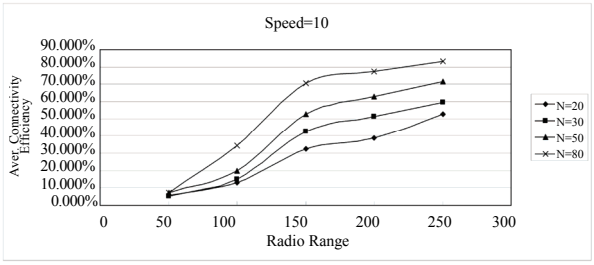

Figure 2. Average connectivity efficiency vs. transmission range for different number of node when speed =10

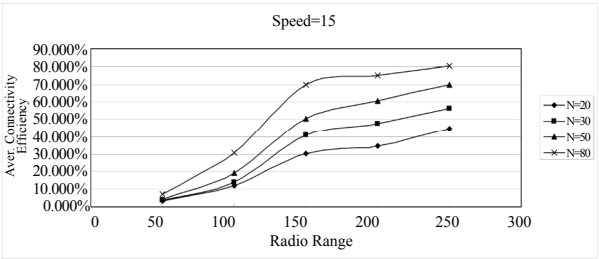

Figure 3. Average connectivity efficiency vs. transmission range for different number of node when speed =15

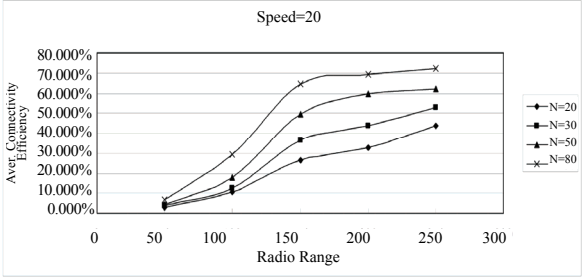

Figure 4. Average connectivity efficiency vs. transmission range for different number of node when speed =20

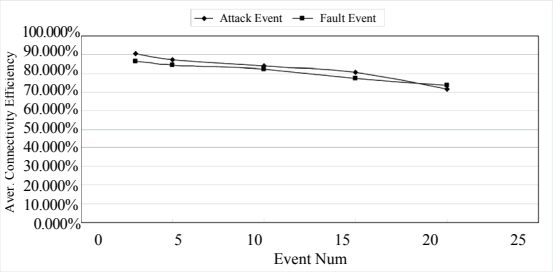

Figure 5. Average connectivity efficiency vs. different event number per minute

In this paper, attacks of network layer, data-link layer and physical layer are the three types of attacks that are included in the experiment. Energy consumption attacks, for network layer attack testing, and jamming attacks, for physical layer attack testing, are selected as examples to test the influences on MANET survivability under attacks. Node mobility is not considered either.

We make the simulation in a 1000*1000 bounded square area under different event frequency, which means we set different number of event that happen per minute. For every minute we choose these events randomly.

Parameters used in the experiment of the influences on MANET survivability of faults or attacks are as follows:

- Simulation time:300
- Average fault/attack amount per minute:3−20
- Node amount:100
- Radio range of each node:100
- Mobile way of each node: quite
- Routing protocol of each node: AODV
- Bandwidth of each link:1Mb

From the results we can find out that when event frequency of faults or attacks increases, more nodes can't provide stable services for routing and forwarding, and the connectivity efficiency decreases.

5. Conclusions and Future Work

In this paper, we systematically analyzed MANET survivability and the impacts that affect it. Based on this, we designed and implemented the simulation environment. The simulation environment represents characteristics of MANET towards survivability and events that impact survivability of MANET like fault events and attack events. We then tested the influences of the above- mentioned impacts under the simulation environment. Users can also configure new topologies, attacks and faults to test MANET survivability in this simulation environment using their own scenario. In our current research, the influences of each factor were tested independently. That means, future work shall be done to present cross-analysis of the influences of these impacts.

REFERENCES

[1] P. Papadimitratos and Z. Haas, "Handbook of ad hoc wireless networks," chapter Securing mobile ad hoc networks, CRC Press, 2002.

[2] F. Adelstein, S. K. S. Gupta, and G. G. Richard III, "Funda-mentals of mobile and pervasive computing," McGraw-Hill, 2005.

[3] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Communications surveys & tutorials, 7(4): pp. 2−28, 2005.

[4] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," ACM SIGMOBILE Mobile Computing and Communications Review, 6(3): pp. 106−107, 2002.

[5] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless personal communications: an international journal, 29 (3−4): pp. 367−388, 2004.

[6] K. Paul, R. R. Choudhuri, and S. Bandyopadhyay, "Survivability analysis of ad hoc wireless network architecture," Proceedings of the IFIP-TC6/European Commission International Workshop on Mobile and Wireless Communication Networks, pp. 31−46, May 16−17, 2000.

[7] J. Short, R. Bagrodia, and L. Kleinrock, "Mobile wireless network system simulation," Wireless Network Journal, Vol. 1, No. 4, 1995.

[8] R. J. Ellison, D. A. Fisher, and R. C. Linger, "An approach to survivable systems," In: NATO IST Symposium on Protecting Information Systems in the 21st Century, 1999.

[9] M. S. Deutsch and R. R.Willis, "Software quality engineering: A total technical and management approach," IST Symposium on Protecting Information Systems in the 21st Century, 1999, Englewood Cliffs, NJ: Prentice- Hall, 1988.

[10] B. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead, "Survivable network systems: An emerging discipline," Technical Report CMU/SEI-97-TR-013, Software Engineering Institute, Carnegie Mellon University, November 1997.

[11] D. Moitrasoumyo and L. K. Suresh, "A simulation model of managing survivability of network of emergent Systems," [J], TechnicalRePort CMU/SEI-2000-TR-020, 2000.

[12] K. J. Sanjay, M. W. Jeannette, and C. L. Richard, "Survivability Analysis of Network Spesifications," In: Workshop on Depended ability Despite Malicious Fault, 2000 Intemational Conefreneeon Dependable Systemsand Networks (DSN2000); 2000, NewYork USA: IEEE ComPuterSoeiety: 2000, June 25−28, 2000.

[13] R. W. Makr, "The quantitative impact of survivable network architectural on service availbaility," [J], IEEE Communications Magazine, 36(5): pp. 71−77, 1998.

[14] D. Y. Chen, S. Garg, and K. S. Trivedi, "Network survivability performance evaluation: A quantitative approach with applications in wireless ad-hoc networks," Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems, Atlanta, Georgia, USA, pp. 28−28, September 2002.

[15] Dahlberg, T. S. Ramaswamy, and D. Tipper, "Issues in the survivability of wireless networks," Proceedings IEEE Mobile and Wireless Communication Networks Workshop, May 1997.

[16] B.Wu, J. M. Chen, and J. Wu, "A survey of attack and countermeasures in mobile ad hoc networks," Wireless Network Security, Springer US, pp. 103−135, 2007.

[17] G. F. Riley, "The georgia tech network simulator," In Proceedings of the ACM SIGCOMM, New York, pp. 5−12, August 2003.

