Survivability in MANETs

Pimal Khanpara, Bhushan Trivedi

***Abstract*—In this paper, we describe the concept of survivability and the issues related to it for Mobile Ad hoc Networks (MANETs). The paper also presents the systematic analysis of the properties and requirements of survivability in the ad hoc environment. The classification and analysis of factors affecting survivability is also given with respect to ad hoc networks. The main categories of such factors are attacks, faults and dynamic topology. The other fundamental characteristics of MANETs are also considered for the study.**

***Index Terms*—Ad hoc Networks, Survivability, Security**

I. INTRODUCTION

Highlight a section that you want to designate with a certain style, and then select the appropriate name on the style menu. The style will adjust your fonts and line spacing. **Do not change the font sizes or line spacing to squeeze more text into a limited number of pages.** Use italics for emphasis; do not underline. Mobile Ad hoc Networks (MANETs) are infrastructure-less, self-organizing wireless networks which consist of mobile nodes in the absence of any centralized management entity [1]. Wireless nodes in MANETs use air as the communication medium and also act as routers. There are many practical applications where MANETs can be used as communication means. For instance, they can be used in military communications to build a network in battlefield without any designated infrastructure. MANETs can also be used in civilian communications such as meetings or conferences. Absence of infrastructure, mobility of nodes, dynamic topology and limited resources are the basic characteristics of MANETs.

MANETs are expected to provide services in diverse conditions. Due to this requirement, survivability in MANETs becomes very demanding. Fundamental characteristics of MANETs make them vulnerable to a variety of attacks and intrusions. Non-malicious faults also cause failures of network services in MANETs. Malicious attackers usually target the basic operations and services in the network and attempt to disrupt them. These operations and services may differ based on the specific applications of MANETs.

To provide the very basic services and keep the fundamental network operations intact in MANETs, it is important to build the ability of surviving attacks. Survivability as the concept was first proposed by Barnes in 1993. After that, many researchers and organizations have put efforts to achieve survivability in the given systems. Survivability can be defined as the capability of a system to offer essential services in timely manner even in the presence of accidents, attacks or failures. Current research work in MANETs also focuses on designing survivable protocols for the given applications and embed them into the existing networks [2]. However, there are only a few such integrated protocols are available for ad hoc networks [2]. Survivability in MANETs depends on the network attributes, routing protocols, attacks, faults, applications and other simulation parameters chosen for conducting experiments. The evaluation of survivability may not be the exact due to the general limitations of simulators used. Moreover, the threat models chosen for inducing accidental or malicious faults and attacks are also not perfect when they are brought into specific simulation environments.

For all these reasons, we attempt to present a complete and systematic analysis of survivability in mobile ad hoc networks. This paper first describes the general concept of survivability for systems. We then present the idea of survivability in ad hoc environment and the related issues. We also describe the attributes and parameters affecting survivability in MANETs. The desirable properties and requirements of MANETs towards achieving survivability is also given.

II. THE CONCEPT OF SURVIVABILITY

The concept of survivability is derived from the term dependability. Dependability is a measure of reliability, availability and maintainability of a system. Sometimes, other characteristics such as security, durability, safety and performance are also considered to evaluate dependability. Dependability is application-specific and can generally be defined as the ability of a system to provide services that can be justified within a time period [3]. Some research works also emphasize on the mechanisms required to improve and maintain the dependability of the given system.

Survivability can be considered as a special case of dependability. The main focus in survivability is on the fault tolerance feature of dependability. The concept of survivability has been introduced as a framework for developing requirements and mechanisms for achieving dependability [3].

Originally, the concept of survivability was first given in the context of military applications. It was defined as a system's or equipment's characteristic that defines a degree of assurance that a given system or equipment is functional under any circumstances. Variants of this definition is given by researchers by considering different service attributes and

Manuscript received Dec, 2017.
***Pimal Khanpara,** Department of Computer Engineering, Nirma University.*
***Bhushan Trivedi**, GLS University, Ahmedabad, India.*

parameters. In general, survivability is defined as the ability of a system to fulfil its mission in a timely manner and in the presence of attacks, accidents or failures [4]. It has only one objective, which is to provide services in timely manner even in critical situations. Some definitions focus on recovery of all services while others only consider the fulfilment of mission [3]. There is no clear boundary between the relationships between services, functions and mission. Services of the survivable systems should have the capability of resisting and recognizing intrusions and attacks, recovering from them and adapting themselves in the presence of intrusions or attacks to lower the impact of future attacks. To decide whether a system is survivable, it is needed to first determine whether operations and services offered by the system are available in a hostile environment. For that, the services are to be classified as essential and not essential. Moreover, the essential services expected from the system should be assigned levels of operations and priorities. In [5], the steps of defining survivability strategy are given. According to that, three major steps are required: Prevention, Detection and Mitigation with recovery. The requirements considered are mainly system's survivability requirements, application-specific intrusion requirement, functional requirements, development requirements, and evolution requirements [6]. The concept of survivability is applicable to the entire system that provides defined services and not to any specific component or part of the system. The main objective is to fulfil the mission, particularly performance of essential services rather than recovery of full services. A survivable system must first resist the attacks attempting to target the system. If they are not successful in that, they should react and try to recover from the impact caused by the attack to avoid a complete breakdown of the system. To make the system survivable in the hostile environment, either capabilities of the system can be reduced so that a system can function or the system can be made to function for a duration in which specified essential services are provided. As survivability is similar to dependability, it also has attributes as safety, security, reliability, availability and fault tolerance [4]. To balance these attributes, services are required to be prioritized in a survivable system.

Survivability was first presented as a concept by Bames in 1993. However, all-acceptant survivability definition is not available until now. The definition given by a research group CMU/SEI, is considered the most influencing so far. According to this definition, survivability is defined as the ability of a system to fulfil its mission in a timely manner, in the presence of attacks, failures and accidents [7]. Many other definitions of survivability are available as per the perspective of different researchers in different areas. In software engineering, survivability is defined as the degree to measure the durability of the system. Here, the basic objective is to check which essential functions or operations are still available even when some part of the system is not functional [8]. Another definition of survivability given by Ellison et al. describes it as the capability of a computing system to offer essential services in the presence of attacks and failures, and recover all services in a timely manner [6]. Many other researchers like Jha and Wilson [9] also defined survivability in a similar manner.

Definitions given above explain the general meaning of survivability in different areas, but they do not specify the attributes and requirements of survivability in the given domain, especially for ad hoc networks. To describe survivability in a better way, formal definition of survivability in mobile ad hoc networks is required.

III. THE CONCEPT OF SURVIVABILITY

After the analysis of survivability definitions given above, we understand that the basis of survivability is the ability of providing essential services at the system level. In [1] [10] [11], essential services that a MANET needs to provide are listed. Out of all these services, network communication is considered as the basic service which must be provided by the network. In general, essential services to be provided by a survivable system primarily depend upon the fundamental requirements of the given system. For a mobile ad hoc network, establishing and maintaining a connection between two nodes at any time; and transmitting packets over available links to complete the required communication are considered as the essential services to achieve survivability. Therefore, survivability of a MANET depends on how well the network provides these services and what the network demands for fulfilling it. The basic characteristics of MANETs also have the impact on survivability. Following are the major characteristics of mobile ad hoc networks which are very important consider for making networks survivable:

A. Node Mobility and Network Topology

Nodes participating in mobile ad hoc networks can move freely. They can enter or leave the network any time. As a consequence of this, MANETs do not have fixed network topology. It changes randomly with the movement of nodes, resulting into a dynamic topology.

B. Faults and Failures

In MANETs, faults can happen in communication links or network nodes. For example, a node may fail for certain reasons such as power failure or lack of computational resources. Communication links may be influenced by an attacker or obstacle.

C. External or Internal Attacks

MANETs use air as the communication medium. Wireless links and participating nodes are not protected and hence can be targeted by external attackers. An attack in MANETs can also be generated by the participating nodes internally. Functionalities of different layers of a mobile ad hoc network are influenced by external or internal attacks. The blackhole, grayhole, wormhole etc are the attacks that target a MANET at the network layer. Eavesdropping and jamming attacks are common to be encountered at the physical layer. At the transport layer, SYN flooding attack usually occurs.

By considering the above threats of mobile ad hoc networks, we can re-define the concept of survivability as the

capability of establishing a communication service between any two participating nodes in the network at any time even when the above threats are present in the network.

IV. MORE ON SURVIVABILITY IN MANETS

Based on the definitions of survivability listed above and considering the factors affecting the survivability in ad hoc environment, the issues related to MANET survivability are classified as: the fundamental properties of ad hoc networks, the impact of these properties on survivability and the basic services that an ad hoc network must provide. Further analysis of these is given below.

Let us denote a mobile ad hoc network as MADhNet. The services which are considered essential are denoted as EssSer.

The characteristics of ad hoc networks affecting the survivability are represented as IMPACT. Thus, a survivable mobile ad hoc network can be defined as,

SurvMANET : = {MADhNet, EssSer, IMPACT}

A mobile ad hoc network consists of a number of participating nodes with certain attributes and properties related to ad hoc communication and survivability. The following are the node attributes in MANETs: IP address, mobility type, radio range, energy level, protocol type, state and location of the node. All these attributes are important consider for survivability in mobile ad hoc networks. The relationship between all these attributes and survivability of mobile ad hoc networks can be described as below.

MADhNet : = {Nodes, Links}
Nodes : = {Set of Network Nodes $node_1$, $node_2$, …, $node_k$}
Links : = {Set of links between $node_i$ and $node_j$}
node : = {ip_address, mobility_type, radio_range, energy_level, protocol_type, state, location}

One of the required essential services in mobile ad hoc networks is to establish routes between any two nodes and transmit packet to complete the process of communication at any instant. There are two steps involved in establishing a connection in an ad hoc network. First, connections are established between any two nodes who wish to communicate by the physical layer and the data link layer. Such connections are then extended by the upper layer, the network layer from one hop to multiple hops. In general, we can say that for a mobile ad hoc network with k nodes, it is required to establish a directional route between any two nodes. This route may include multiple nodes in it. Such a route must follow the below constraints:

- Any node along this route must have an entry in its routing table for the destination node and next node on that route.
- The distance between any two neighboring nodes $node_i$ and $node_j$ is not greater than the transmission range of $node_i$.

The fundamental characteristics of mobile ad hoc networks which have a great impact on the survivability of networks are node mobility, dynamic topology, attacks and faults. The essence of all these factors is to disrupt the process of communication by destroying the route between the communicating nodes. The end objective of implementing survivability is save the network from being disconnected. We can describe these characteristics and their impact as,

IMPACT : = {Node_Mobility, Dynamic_Topology, Faults, Attacks}

The main reason behind dynamic topology in mobile ad hoc networks is the mobility of nodes. Nodes move randomly and rapidly in such network and this causes the topology of the network changing frequently. When nodes move in the network, their locations are changed. Due to this, the necessary distance constraint at the link layer may not be satisfied. When topology changes due to node movement, it happens that the distance between the two neighboring nodes along the newly found route, is greater than the transmission range of the first node. As this condition violates the required constraint, the route is dropped. If all other available routes fail due to the same reason, the communication between the source node and destination node cannot take place.

Faults in mobile ad hoc networks are usually due to faults in network nodes and communication links. Faults in network nodes occur when the state of the nodes are changed to “down” due to accidental or malicious actions. If the state of a network node is set to down, the node cannot be included in any communication path. It also changes the range of transmission of the node to 0, violating the basic constraint. Due to these, the route involving that node becomes invalid and cannot be used for further transmissions. Link faults occur due to obstacles between nodes. Sometimes, link fault is also caused by influencing the node transmission range by fading effect of signals. These faults can be described as below:

Fault : = { Node Faults, Link Faults}

In mobile ad hoc networks, there are different criteria to categorize attacks. Attacks can originated inside the network by the compromised participating nodes. Such attacks are known as internal attacks. Attacks imposed by malicious entities which are not a part of the network, are called external attacks. The layered infrastructure of ad hoc networks is important to consider to find the effect of attacks layer-wise, on specific network functionalities. Attacks which target the topmost layer of a mobile ad hoc network, the application layer, are mostly similar to the ones targeting the wired network. The main goal of such attacks is to disrupt the application services. At the transport layer, actions that attempt to disrupt the functionalities of transport layer protocols are treated as attacks. SYN flooding is one of the commonly found transport layer attack. The network layer becomes the target of many attackers as important network functionalities such as routing are implemented at this layer. Attackers usually aim at destroying routing and data

forwarding processes at this layer. At the data link layer, attackers attempt to destroy the link connections between adjacent nodes. Attackers try to implement eavesdropping, jamming or interception attacks on the wireless medium at the physical layer. Attacks impacting the survivability of mobile ad hoc networks can be described as follows:

Attacks : = {Application_Attack, Transport_Attack, Network_Attack, DataLink_Attack, Physical_Attack}

V. CONCLUSION

The systematic analysis of survivability in mobile ad hoc environment is presented in detail in this paper. The important characteristics of mobile ad hoc networks affecting the survivability property of such networks is considered to define survivability for MANETs. The influence of other events that causes a change in the ability of a mobile ad hoc network of surviving the effects of various faults, errors and attacks is also presented. Our current research focuses on developing a general survivability framework for existing mobile ad hoc networks, based on the factors, attributes and actions discussed above in this paper.

REFERENCES

[1] P. Papadimitratos and Z. Haas, "Handbook of ad hoc wireless networks," chapter Securing mobile ad hoc networks, CRC Press, 2002.
[2] 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.
[3] 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.
[4] 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.
[5] D. Moitrasoumyo and L. K. Suresh, "A simulation model of managing survivability of network of emergent Systems," TechnialRePort CMU/SEI-2000-TR-020, 2000.
[6] 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, November1997.
[7] Dahlberg, T. S. Ramaswamy, and D. Tipper, "Issues in the survivability of wireless networks," Proceedings IEEE Mobile and Wireless Communication Networks Workshop, May 1997.
[8] 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.
[9] 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.
[10] F. Adelstein, S. K. S. Gupta, and G. G. Richard III, "Funda-mentals of mobile and pervasive computing," McGraw-Hill, 2005.
[11] 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.
[12] 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.