RESILIENCE AND SURVIVABILITY IN MANET: DISCIPLINE, ISSUE AND CHALLENGE

A.H Azni[1], Rabiah Ahmad[2], Zul Azri[3]

[1,2,3]Universiti Teknikal Malaysia Melaka, Malaysia,
[1]ahazni@gmail.com,[2] rabiah@utem.edu.my, [3]zulazri@utem.edu.my

ABSTRACT. The wireless technology has become essential part in modern life, and thus the consequences of network disruption is becoming severe. It is widely known that wireless network is not sufficiently resilience, survive and dependable and significant research and development is necessary to improve the situation. This paper provide a survey of vast disciplines in MANET, a resilience strategy is also presented on how to defend, detect and countermeasures malicious node. Current issues and challenges to achieve resilience and survivability is also presented for future direction

Keywords: wireless technology, MANET

INTRODUCTION

The usage of wireless technology has tremendously increased due to rapid proliferation of wireless lightweight devices such as laptops, PDAs, wireless telephones, and wireless sensors. They have been used in applications such as survivable, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. These applications demand high security protection and resilience where any weaknesses identified needed to be addressed appropriately. In Mobile Ad Hoc Networks (MANETs), the nodes are mobile. As a result, the network topology may change rapidly and unpredictably over time. Furthermore, the network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves.

The dependency on mobile ad hoc application has gained interest to many industries. However, the increase dependencies on these sophisticated services make wireless network more vulnerable to problems. This will results in increasing consequences of disruption and becoming more attractive to attacks. Current research in MANET mainly focuses on routing problems but did not include resilience and survivability in their protocol design (Fei Xing, 2010). Resilience defines by P.G. James and H. David is the ability of the network to provide and maintain an acceptable level of services in the face of various faults and challenges to normal operation (P.G. James, 2010). This paper focuses on a broad overview of resilience and survivability concept in MANETs. Rest of this paper is organized as follows: section II present resilience and survivability discipline in MANETs. Section III will discuss resilience issues and mechanism. Section IV presents strategies for achieving network resilience and survivability in MANETs. Finally we conclude and present our future direction.

RESILIENCE AND SURVIVABILITY DISCIPLINES

Resilience covers broad disciplines in MANET. Figure 1 show disciplines of resilience in MANET, which is divided into two categories, tolerance and trustworthy.

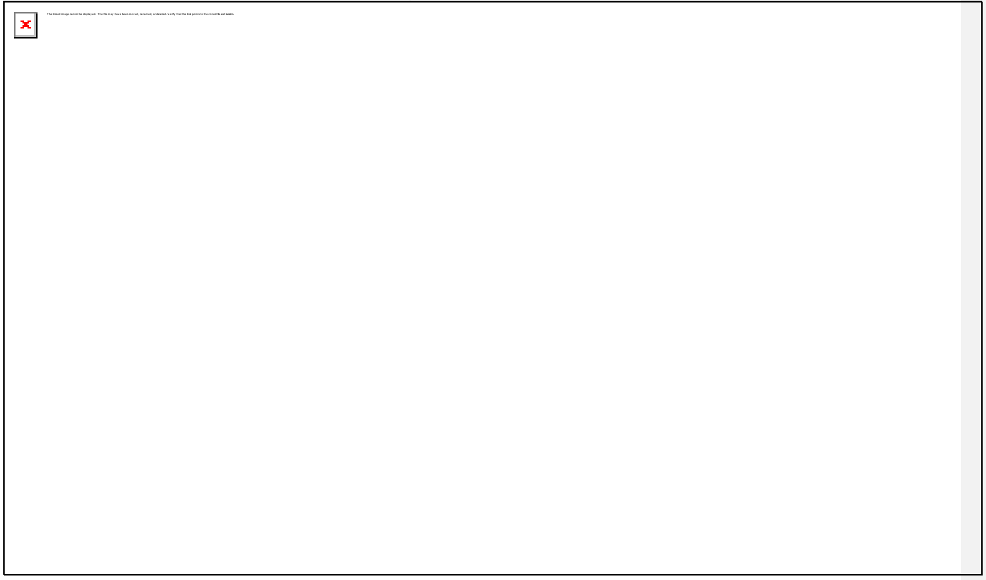
The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Figure 1: Resilience Discipline

It covers the area of survivability, intrusion and fault tolerance, dependability, security and performance (Sterbernz, 2010). Each discipline has a basis of action as part of resilience strategy. The first discipline is tolerance which can be define as how the systems react, counterpart, recover and allowed intrusion or failures at a tolerable rate to prevent it from generating system failures (Michele Nogueira Lima, 2009). The concept of tolerance comes from two classical areas of computer science which are fault-tolerant and intrusion-tolerant. However, intrusion tolerance in MANETs just started recently after the application on wireless mobile becomes wide spread. Techniques for tolerance can be classified as redundancy, recovery and replication.

- **Redundancy** can be achieved using multiple route paths in routing protocol. This technique uses multiple paths to transmit identical copies of the packets in each path to avoid packet loss in the case of attacks. In case the channel been attacks, the packets can be recovered from other sources.
- **Replication** uses technique to replicate the key and assume that the system operates correctly only if *f* out of *n* of its replicas is compromise.
- **Recovery** is the capability of restoring disrupted information or functionality within time constraints, limiting the damage and maintaining essential services.

Survivability in the context of MANET classified as tolerance concept. It refers to the capability of a system to fulfill its mission in a timely manner at the present of threats or failure (Yuan Zhou, 2009). It involves correlated failure of nodes due to attacks or network disruption. Survival properties are resistance, recognition, recovery and adaptability (Michele Nogueira Lima, 2009). Resistance is the capability of a system to repel attacks via user authentication, firewalls and cryptography. Recognition is the system capacity to detect attacks and evaluate the extent of damage. Recovery is the capability of restoring disrupted information or functionality within time constraints, limiting the damage and maintaining essential services. Conventional strategies applied for achieving recovery are replication and redundancy. Finally, adaptability incorporating lessons learned from failures and adapting to emerging threats

The second discipline categories under the area of trustworthiness. It defines as assurance that a system will perform as expected (Pradeep Rai, 2010). The trustworthiness measures service delivery of network which are dependability, security and performance. In MANET, nodes are depended on other node(s) to route or forward a packet to its destination via wireless medium. Thus, nodes in MANET required highly reliability and availability of networks. Security is crucial in MANETs especially when it is involved highly sensitive transmission. In general, security mechanism in MANET follows two defense lines: one preventive and another reactive (Jie Li, 2008). The prevention is the first line of defense which protects the network form external. It is mainly achieved by securing routing protocols which prevent the attacker from installing incorrect routing updates at other nodes. On the other hand, reactive is the second line of defense which protects the internal attacks. It roles is to take action on demand to mitigate intrusion, it is actually act like intrusion detection systems (IDS). The last discipline in resilience is to measure performance of MANET. Performance refers to property of system that measures quality of services (QoS) such as delay, throughput or goodput, and packet delivery ration (Lee Bu Sung, 2003).

RESILIENCE ISSUES AND CHALLENGES IN MANET

This section describes current issues and challenges to MANET that motivate the need for resilience. MANET defined above as connected nodes which form dynamic topology without centralized operation. Unlike wired, nodes in MANET performed all routing activities within the node itself. Due to that, MANETs are more vulnerable to failures compared with wired networks due to topology changes, node misbehaviors, or even security attacks, which imposes a critical demand for the resilience of these networks.

The concept of resilience in MANET should guarantee the communication network between sender node and receiver node even if some of their hopping terminal failed or out of service area. Therefore the issue against nodes misbehavior and failures is critical to resilience-oriented applications. There have been a number of researches proposed to tackle resilience issues in MANET. Most of the researches proposed are solution to enhance QoS, ensuring data integrity and availability. However, issues on nodes misbehavior, security attacks and node failure is limited. The researchers also assume that nodes in MANETs are treated independently when it comes to measure impact analysis of the network.

In real situation, nodes in MANET should be correlated with each other. For example, if a node has more and more neighbors failed, it may need to load more traffic originally forwarded by those failed neighbors, and thus nodes might become failed faster due to excessive energy consumption. Similarly, it is also possible that the more malicious neighbors a node has, the more likely the node will be compromised by its malicious neighbors (Xing, 2009). This scenario will affect network resiliency in MANETs. Thus, it is important to look at the issues how these correlated behaviors will affect the network resilience in MANET. Various node misbehaviors will also affect network resilience in MANETS. The most important is its topological connectivity and delay-throughput. At this moment, current research still lacks of quantitative analysis to measure the impact of network resilience. It is good that if we can model and analyze the network impacts quantitatively based on a specific resilience metric mention above in the consideration of correlated node misbehaviors.

The challenges to the above issues come from random mobility pattern of the nodes, resources constraint, and malicious attacks. Network topology in MANET changes over time due to its random mobility pattern. The solution to the above issue must be self-adjustable to dynamic topology changes as well as node behaviors. Furthermore, MANET also has its limitation in terms of it energy resources and bandwidth constraint. Most devices in MANETs are battery operated, thus, the solution should consider a low communication overhead and computational complexity. Another big challenge to MANETs is advance malicious nodes such as Dynamic DOS attacks. It is very difficult to detect the presence of attacks via node misbehaviors.

STRATEGIES TO ACHIEVE NETWORK RESILIENCE AND SURVIVABILITY IN MANET

Resilience and survivability in MANET required state-of-the-art strategies to maintain connection topology in the presence of attacks or random failures. In general, conventional survivability strategies rely on redundancy and replication to use the best route for data transfer in order to achieve network performance. To ensure the network achieve the objective of the services, for availability and reliability, redundancy techniques such as in routing discovery used multiple paths routing protocol to provide redundancy in data transmission. Multiple path routing protocols can use all routes found simultaneously and transmit the same data more than one time or can use them on demand or as an alternative. On the other hand, in security, replication technique uses to protect data confidentiality. Redundancy techniques such as certificate authority scheme (Foyer, 1999) can be applied by dividing the key into part and distributed among the nodes. The nodes will have replicates keys in case some of the keys have been compromised. Other techniques can be used is to split messages into pieces by the source node. Each of the messages is encrypted and sent out via multiple independent paths.

In quantitative approaches, survivability in MANETs is modeled and analyzed mathematically. Based on the model, the impact of network survivability can be measured according to specific resilience metrics. Moreover, various nodes behavior also can be analyzed quantitatively and how the nodes behavior will affect network resilience. The most important is its topological connectivity and delay-throughput. At this moment, current research still lacks of quantitative analysis to measure the impact of network resilience.

CONCLUSION

Wireless technologies have become essential to all aspect of modern life, and thus the consequences of network failure have become increasingly severe. It is widely recognized that wireless network is not sufficiently resilience, survivable or reliable. The researches in these areas are extremely important to improve network performances and services. There are many possible promising future directions in the broad topic of resilience as discuss above and problem in dealing with correlated nodes behavior and how it affect network resilience in MANET discussed elsewhere. However, modeling correlated node behaviors itself can be even more challenging task and really require urgent further research.

REFERENCES

F.Xing, W.Wang (2010). *On the survivability of wireless ad hoc networks with node Misbehavior and Failure,* IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 3, July-September 2010, 284-299

Foyer, C. P. (1999). Ad Hoc On-Demand Distance Vector Routing. *2nd IEEE Workshop,Mobile Computer Sys. And Apps,* .

Jie Li, R. L. (2008, April). Future Trust Management Framework for Mobile Ad Hoc Networks IEEE Communications Magazine. *IEEE Communications Magazine* .

Lee Bu Sung, W. K. (2003). Performance of Mobile Ad Hoc Network in Constrained Mobility Pattern. *2003 International Conference on Wireless Networks*. Las Vegas, Nevada, USA: CSREA Press 2003.

Michele Nogueira Lima, A. L. (2009). A Survey of Survivability in Mobile Ad Hoc. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 1* , 66-77.

Pradeep Rai, S. S. (2010). A Review of ‘MANET’s Security Aspects and Challenges'. *IJCA Special Issue on “Mobile Ad-hoc Networks”* , 162-166.

Smith, P., (2010), *Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines*, Computer Networks Volume 54, Issue 8, 1 June 2010, Pages 1245-1265, Retieve from http://www.sciencedirect.com

Sterbenze, J.P.G, Hutchinsion, D., Cetinkaya, E.K, Jabbar, A., Rohrer, J.P, Scholler,M.,

viors and failures. IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 3, 284-299. Retrieve from http://www.ieee.org

Xing, F. (2009). Modeling, Design, and Analysis on the Resilience of Large-scale Wireless Multi- Hop Networks. Raleigh, North CArolina, USA: Department Of Engineering, North Carolina State University.

Yuan Zhou, C. X. (2009). Research on Survivability of Mobile Ad-hoc Network. *Journal Software Engineering & Applications* , 50-54.