A Survey on the Detection, Mitigation and Security Model for Disruption Tolerant Network

P.Rajalakshmi[1], Dr.C.Sundar*[2]

[1]*PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*
chitradevi9106@gmail.com

[2]*Associate Professor, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*
sundarc007@yahoo.com

**Corresponding Author*

Abstract— **In adversary environments most popular connection scenarios between with each other and access the confidential information. The enforcement of authorization policies using DTN technology are becoming successful solution for composed of intermittently on military networks. In environments which are meant to those connected nodes. In a DTN with a malicious node transmit to its destination..Such as includes bulk of data and no involved on the military networks. In this paper to introduce RWG framework (GSF) for survivability in ICMANETS. GSF aim to survive the system detection, diagnosis and mitigation. RWG protocol to exploiting the external storage node. This survey entitles the above problem and solution is proposed.**

Keywords— **DTN, GSF, RWG Framework .**

I. INTRODUCTION

To securely and efficiently manage in the disruption tolerant adversary environment. In DTN technology most popular for military network, In this technology after more than ten years of active research in the field, recent developments in the field, recent developments in the field and highlight those areas with high for future development. reviewed recent advances in developing DTN software, application and services. The DTN implementations achieve in sufficient performance for most scenarios. A killer application for DTN is yet to be found [1].

A DOS is the disruption of services by control access to a system or service instead of overthrowing the service itself. attacks aimed preventing and assuring the correct message delivery in structured peer to peer overlays and defences to these attacks are discussed [2], complexity in routing increases their random walk gossip protocol, which uses an efficient data structure to keep track of already informed nodes with minimal signalling, avoiding unnecessary transmissions[3].RWG can be following some characteristics:

- Deal with intermittent connectivity by partition tolerance.
- Bandwidth and energy efficient in the sense of few transmissions per data packet.
- A reasonable average latency.

RWG protocol is being able to handle much higher loads [3], plan to further mathematically analyze the protocol to see if it is possible to drive bounds on latency[3]. DTN is a intermittently maximum time there does not exist a clear way from source to the destination[4]. In this methods are implemented to improve the forwarding techniques and reduce the end to end delay in this type of network is still a challenging one[4]. DTN transfers data using a store mechanism in this nodes reduces the packet delivery ration and waste system resources[5]. It does not rely on any specific routing algorithm. A framework for monitoring a disruptive attacks based upon a network security. It includes a group of function to detection, diagnosis and performs mitigation Not resistant to multiple attacks in time intervals.

II. DISRUPTION TOLERANT NETWORK

A DTN is a network designed for the temporary or intermittent communication problem, limitations have their adverse impact of least possibilities. There are several aspects to the effective design including:

- The use of fault tolerant methods is to increase the redundancy in network by having high tolerable performance.
- The quality of graceful degradation under adverse condition or extreme traffic loads. This is used to prevent or quickly recover from electronic attacks. Ability to function with minimal latency even when routes are

well defined or unreliable

Fault tolerant: fault tolerance is the way in which an operating system responds to a hardware or software failure. The term essentially refers to a system's ability to allow for failures or malfunctions, and this ability may be provided by software, hardware or a combination of both. To handle faults gracefully. some computer systems have 2 or more duplicates system..

Graceful degradation: Graceful degradation is always plays an important role in large networks. Resisting massive physical as well as electronic attacks may happen in communication network. In this system architecture, if continues on working in some extent even though a large portion of it has been destroyed .

Electronics attacks: Electronics attacks on networks can take in the form of viruses, worms, Trojans, spyware and other destructive programs or codes. Here, network servers have some schemes that includes denial of service attacks and malicious attacks. In some instance, malicious hackers commit acts on identity the data theft against individual subscribers or the groups of subscribers in an attempt to uncoveraged network use.

Minimal latency: As the network and their usage criteria's may differ, routes can be modified within second. Due to this delays of temporary propagation, the caused latency is unacceptable. Data transmission is also blocked altogether. In a DTN, their frequency_events are kept as minimum as possible.

III. Security Model

A security model that provides a convincing case for the robustness of DTN's, this model includes several elements they are,

- Identity
- Routing Security
- Knowledge
- Mobility

A . Identity

DTN environment without authentication, no assumptions can be made about the identities of other peers.

B. Routing security:

This model only evaluates the security of the routing itself. Routing may be accomplished without authentication this does not need for end to end authentication and confidentiality mechanism.

C. *Knowledge*

We distinguish between week and strong attackers. Nodes are chosen to be weak attackers uniformly at random to simulate an opportunistic attack in real wired or wireless network. In contrast, strong attackers have knowledge of the complete network topology which is likely to be more information than any node would have in practices.

D. *Mobility:* An attacker can follow any mobility pattern and attack all nodes that move within wireless range, or can remain permanently within range of one node in the network.

IV. General Survivability Framework(**GSF)**

Attack modalities: To determine how the network performance of a DTN degrades when no authentication protocol is used.

Attacks types: This security model a number of attacks are possible. We focus on a set of actions that are fundamental to any attacks. These four actions are detailed, they are

- Dropping all packets
- Flooding of packets
- Routing tale falsification Counterfeit
- Acknowledgments of delivery.

A. *Dropping packets*: The simplest attack a node can delivery involves dropping all packets that it receivers. This attack can be devastating to network performance when a dropping node is a commonly used path. For forwarding protocols every dropped packet is a lost packet. The best defence in a DTN against malicious packet dropping attacks is the use of multiple paths.

B. *Flooding:* A flooding attacker continuously sends fake data destined for any node, sourced from any node and bearing arbitrary header flags. In a wired network, flooding attacks are the basic of much denial of attacks. DTN flooding is much less effective because a direct route to a destination is not always available

C. *Routing table falsification*: Traditional networks are often susceptible to injection of erroneous routing information. This can cause routers to delay or lose packets altogether, table updates are integrated in to a nodes routing tables if they are dated more recently than those tables the node currently using.

D. *Acknowledgments counterfeiting:* Acknowledgments are a very effective mechanism for packet delivery in replicative routing protocols and as a result, they are an effective method for sabotage. To defend against this attack without authentication, we leverage the fact that packets should normally propagate from nodes closest to a packet source to nodes closest to a packets destination.

V. DETECTION, DIAGNOSIS AND MITIGATION

A. *Detection:* The detection component implemented is a statistical anomaly detector. It will raise an alarm if a given set of observations deviate too much from what is considered normal. The statistical approach has a small footprint the resource constrained context of mobile device. Diagram:

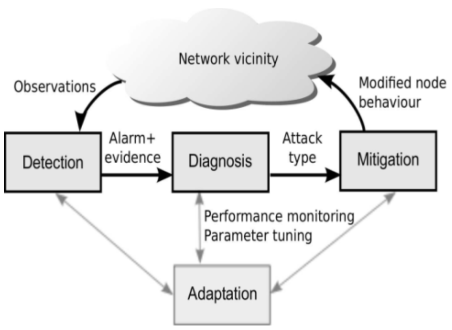

Fig. 1. General Survivability Framework (GSF)

B. *Mitigation*: The mitigation component receives the results from the diagnosis component selects a suitable action as a response to the suspected attack. The component includes a number of mitigation actuators and a mitigation manager.

C. *Diagnosis*: The diagnosis is based on a geometric interpretation of the features that describe the status of the node at a given time. This assumes that the effects of a particular attack in the m-dimensional space are always of the same nature irrespective of the location of the nodes and the conditions of the network.

VI. CONCLUSION

This proposed system can be applied GSF to survive the system attacks mitigation. But we focus mainly for advisory network to secure data communication As area networks such a way it would be the perfect store and forward using military network.

REFERENCES

[1] Atomies, G.voyiatzis, "A Survey of Delay and Disruption-Tolerant Networking Applications", IEEE member, *Journal of Internet Engineering*, vol.5, No.1, june2012.

[2] A.Viswanathan, Ardra.P.S, "A Survey on Detection and Mitigation of Misbehavior in Disruption Tolerant Networks", IRACST-*International Journal of computer networks and wireless communications* (IJCNWC), ISSN: 2250-3501 vol.2, No 6, december2012.

[3] Michael Asplundh, Simon Nadjm-Dehrani "A Partition-tolerant Many cast Algorithm for Disaster Area Networks", Department of computer and Information Science, *Linkoping university*, SE-581 83 Linkoping, Sweden.

[4] D.S. Dolphin Hepsiba et al., "Secured Data Forwarding Technique in Disruption Tolerant Networks-Survey", *International journal of Advanced Research in computer and communication Engineering* vol.3, issue 2, February2014.

[5] AarthyD.K, C.Balakrishnan "Detecting Selfish Routing and Misbehavior of Malicious node in disruption tolerant networks", *International Journal of Emerging Technology and Advanced Engineering,* vol.3, special issue 1, january2013.

[6] Jody cucurull et al., "Surviving Attacks in challenged Networks", *http*://dx.doi.org/10.1109/TDSC.2012.67

[7] John Burgess et al., "Surviving Attacks on Disruption-Tolerant Networks without Authentication", Dept of computer science, *univ.of Massachusett*s, Amherst, USA.

[8] Sharon Goldberg et al., "Path-quality Monitoring in the presence of Adversaries", *Princeton university*, Princeton, NJ 08544.

[9] M.chuah, R.Metzer "Secure opportunistic Data Retrievals in challenged Environments", *Lehigh university*.

[10] M.chuah, J.Han "Performance Evaluation of Information Retrieval Schemes for Multi-Attrite Queries in DTNs", *Lehigh university.*

