Malicious Node Detection in Delay Tolerance Network

Er. Ashu Garg[1], Sourav[2]

[1]Assistant Professor, Department of CSE, JCDM College of Engineering, Sirsa, Haryana, India

[2]M.Tech. Scholar, Department of CSE, JCDM College of Engineering, Sirsa, Haryana, India

ABSTRACT

Delay tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information, and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears. This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion.

We aim to evaluate the added effect of the presence of malicious nodes on ad hoc network performance, and determine appropriate measures to detect malicious nodes. A malicious node advertising itself as having a valid route to the destination. With this intension the attacker consumes or intercepts the packet without any forwarding. An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped. Let H be a malicious node. When H receives a Route Request, it sends back a Route Reply immediately, which constructs the data and can be transmitted by itself with the shortest path. So S receives Route Reply and it is replaced by H->S. then H receives all the data from S. In this research we propose a new assesment based scheme for detection of Malicious Nodes in DTN. And examine different strategies for prevention to malicious nodes as well as Compare out come proposed scheme with the earliest established schemes.

Keywords: Delay tolerant networks, store-carry-and-forward

I. INTRODUCTION

In a wireless network, the routers are responsible for forwarding packets in the network and hosts may be sources or sinks of data flows. Recently many network researchers are studying networks based on new communication techniques, especially wireless communications. Wireless networks allow hosts to roam without the constraints of wired connections. People can deploy a wireless network easily and

quickly. End users can move around while staying connected to the network. Wireless networks play an important role in both military and civilian systems. Handheld personal computer connectivity, notebook computer connectivity, vehicle and ship networks, and rapidly deployed emergency networks are all applications of this kind of network. Hosts and routers in a wireless network can move around. Therefore, the network topology can be dynamic and unpredictable. Traditional routing protocols used for wired networks cannot be directly applied to most wireless networks because some common assumption are not valid in this kind of dynamic network. For example, one assumption is that a node can receive any broadcast message sent by others in the same subnet. However, may not be true for nodes in a wireless mobile network. The bandwidth in this kind of network is usually limited. Thus, this network model introduces great challenges for routing protocols.

II. BEHAVIOUR OF MALICIOUS NODE

If malicious nodes are present in a DTN, they may attempt to reduce network connectivity (and thereby undermine the network's security) by pretending to be cooperative but in effect dropping any data they are meant to pass on. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance. We aim to evaluate the added effect of the presence of malicious nodes on ad hoc network performance, and determine appropriate measures to detect malicious nodes. A malicious node advertising itself as having a valid route to the destination. With this intension the attacker consumes or intercepts the packet without any forwarding. An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped. Let H be a malicious node. When H receives a Route Request, it sends back a Route Reply immediately, which constructs the data and can be transmitted by itself with the shortest path. So S receives Route Reply and

it is replaced by H->S. then H receives all the data from S.

"When a node breaches any of the security principles and is therefore under any attack. Such nodes exhibit one or more of the following behavior:

Packet Drop:- Simply consumes or drops the packet and does not forward it.

Battery Drained:- A malicious node can waste the battery by performing unnecessarily operations.

Buffer Overflow:- A node under attack can fill the buffer with fake updates so that genuine updates cannot be stored further.

Bandwidth Consumption:- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.

Malicious Node Entering:- A malicious node can enter in the network without authentication.

Stale Packets:- This means to inject stale packets into the network to create confusion in the network.

Delay:- Any malicious node can purposely delay the packet forward to it.

Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.

Message Tampering:- A malicious node can tamper the content of the packets. Denying from

Sending Message:- Any malicious node may deny from sending messages to other legitimate nodes.

Fake Routing:- Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations.

Node Not Available:- An intruder can isolate the node from taking part in any operation so as to create delays when the source node chooses another alternative path.

III. LITERATURE REVIEW

Prerana S.Jagadale, Prashant Jawalkar says that Delay/ Disruption Tolerant Networking (DTN) program is an emerging technology that can facilitate access to

information when secure end-to-end paths cannot exist. Disruption tolerant network is a different type of wireless network. It is an intermittently connected mobile network. Delay tolerant network adopts a store carry-and forward mechanism, of which all the participants are assumed to cooperate with one another in message delivery, to overcome the challenges of the intermittent connection and the time-varying network topology.

M. Balaganesh ,P. Sathiya Proposed The survey tries to review the various problems and their solution in Delay Tolerant Network (DTN) while routing the packets. In this paper, going to discuss and see the overview of various methods used in the DTN. They are simbet and bubble rap which are the DTN routing algorithm and is used for identify the bridge nodes using between ness centrality and similarity metrics in the network.

Yanzhi Ren, MooiChoo Chuah said that, The Disruption Tolerant Networks (DTNs) are vulnerable to insider attacks, in which the legitimate nodes are compromised and the adversary modifies the delivery metrics of the node to launch harmful attacks in the networks. The traditional detection approaches of secure routing protocols cannot address such kind of insider attacks in DTNs. In this paper, we propose a mutual correlation detection scheme (MUTON) for addressing these insider attacks.

aser khamayseh, Ruba Al-Salah, Muneer Bani Yassein says that The increased popularity and usage of wireless technologies has oYpened the doors for new emerging applications in the domain of networking. One emerging and promising areas is the domain of Mobile Ad Hoc Networks (DTNs). A mobile ad hoc network is a collection of wireless mobile nodes that form a dynamic network without the need for infrastructure or centralized points. The dynamic nature of ad hoc networks presents many security challenges. Secure routing is a promising area for achieving better security for the network by protecting the routing protocols against malicious attacks. Several secure routing protocols have been proposed in the literatures that were successful in avoiding and preventing some types of security attacks in DTNs. However, DTNs are still vulnerable to other types of attacks.

IV. RESEARCH METHODOLOGY AND OBJECTIVES

Research in common parlance refers to a search for knowledge. Once can also define research as a scientific and systematic search for pertinent information on a specific topic. In fact, research is an art of scientific investigation. The Advanced Learner's Dictionary of Current English lays down the meaning of research as "a careful investigation or inquiry specially through search for new facts in any branch of knowledge."1 Redman and Mory define research as a "systematized effort to gain new knowledge."2 Some people consider research as a movement, a movement from the known to the unknown. It is actually a voyage of discovery. We all possess the vital instinct of inquisitiveness for, when the unknown confronts us, we wonder and our inquisitiveness makes us probe and attain full and fuller understanding of the unknown. This inquisitiveness is the mother of all knowledge and the method, which man employs for obtaining the knowledge of whatever the unknown, can be termed as research.

3.3 OBJECTIVES:-
The main objective of the present work can be stated as –

- To study the different Parameter and Environment of DTN.
- To examine different strategies for prevention to malicious nodes in DTN.
- To propose a new assessment based scheme for detection of Malicious Nodes in DTN.
- Compare the outcome proposed scheme with the existing schemes of malicious node detection.

V. CONCLUSION AND FUTUTRE SCOPE

- From the simulation results, it is found that: the default case is better than Proposed Malicious Node because it has Maximum Packet delivered, Delivery Probability, Minimum Overhead Ratio, and Minimum Average Hope Count.
- For Scenario for various No .Of Nodes. The Conclusion for this Scenario is the Performance of malicious is poor as Comparison to default Max pro Routing.
- In terms of Performance Metrics like as Packet Delivery , delivery probability And overhead ratio the Max pro routing perform Batter as Compared to Malicious Node detection.
- Second scenario waiting time the Conclusion for this Scenario is also same as of the scenario of Various No. Of nodes. In this scenario packet delivery of Max pro routing is higher and the overhead ratio of malicious behavior is high. Higher overhead ratio shows that the performance of malicious behavior is poor.
- Scenario for various node degree at starting, the node degree is zero ,which starting ,the node degree is zero ,which define that all nodes are trusted and the performance good at that time, when   the node degree is increase the performance decreases in term of delivery ratio, delivery probability and overhead ratio at the end of simulation the node are malicious behavior ,so at that time the performance is goes to zero .

So, the final conclusion is that overhead performance of Malicious is poor as comparison Max pro routing

VI. REFERENCES

[1]. https://www.techopedia.com/definition/26186/ wireless-network.

[2]. http://searchnetworking.techtarget.com/feature /Introduction-to-wireless-networks-from-The-book-of-wireless

[3]. https://www.techopedia.com/definition/26186/ wireless-network

[4]. http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html

[5]. http://searchnetworking.techtarget.com/definition/disruption-tolerant-network

[6]. https://en.wikipedia.org/wiki/History_of_delay-tolerant_networking

[7]. http://cse.unl.edu/~wsun/DTNapp.pdf

[8]. https://www.techopedia.com/definition/25927/routing-protocol

[9]. http://www.ijcaonline.org/journal/number17/pxc387557.pdf

[10]. http://www.ijcaonline.org/volume20/number4/pxc3873251.pdf