A SURVEY ON ATTACK DETECTION TECHNIQUES IN DELAY TOLERANT NETWORK

Rajashri Mitharam Chaudhari¹ and Mr. M. P. Patil²
¹² S.S.V.P.S’s B.S.D. College of Engineering, Dhule

Abstract—DTN is a network in which there is no end to end connectivity between source and destination. DTN is characterized by long propagation delay and intermittent connectivity. Due to the limited connectivity, DTN is vulnerable to various attacks, including blackhole and greyhole attacks. Malicious nodes drops all or a part of the received messages, even if they have enough buffer storage. This dropping behavior is known as blackhole and greyhole attacks respectively. This paper provides different types of scheme and their comparison with different parameters. Existing research scheme can detect individual attackers well but they cannot handle the case where attackers cooperate to avoid the detection. The limitation of previous work is that they cannot defend against collusion attacks. Therefore there is a need to develop new attack detection scheme that detects collusion attacks effectively.

I. INTRODUCTION

In Mobile Adhoc Network (MANET) packets can be transferred only if link between the nodes are established. If link is not established then packets will be lost. So packet delivery ratio will be decreased in MANET. To overcome this problem, Delay Tolerant Network (DTN) is used. In DTN each node has some storage capacity. So if the links of nodes are not established then packets will be stored in the storage. DTN is able to provide communication services in unreachable & unfriendly environments.

A DTN is a network architecture that defines a series of contiguous network data bundles that enable applications. In DTN, there is no end to end connectivity between source and destination. DTN is characterized by long propagation delay and intermittent connectivity. DTN is a set of protocols that acts together to enable a standardized method of performing store-carry-forward mechanism. Figure 1.1. shows DTN architecture.

Figure 1.1: DTN Architecture
DTN network has the following several characteristics:
1. **Long delay**
   Long delay between nodes, in addition to variable queuing delays at node buffers, all create end to end path delays.
2. **Limited resources**
3. **Intermittent connectivity**
   If there is no consistent end to end path between source and destination is called as network partitioning.
4. **Asymmetric data rate**
   The Internet does support some forms of asymmetric, bi-directional data, as in cable TV or asymmetric DSL access. But if asymmetries increase then they will hinder traditional interactive protocols such as TCP.
5. **High error rate**
   If bit-errors occur on links, then they either require correction. Hence consuming more bandwidth, or even retransmitting the entire packet, resulting in more network traffic.
6. **No end to end path between source and destination**

II. APPLICATION AREAS OF DELAY TOLERANT NETWORK

There are following application areas of Delay Tolerant Network:

1. **Wild life monitoring**
   This application is concerned with gathering data about wild species and their habits. One of the most famous examples of wildlife monitoring is the ZebraNET project conducted in Sweetwaters Reserve, Kenya. Here, zebras are equipped with custom tracking collars (nodes) and carried across a large wild area. The collars include GPSs, flash memory, wireless transceivers, and a small CPU.

2. **Underwater sensors**
   In this application, medium of transmission is water. RF communication generally does not work in water. In such cases and due to the nature of the location, nodes (mobile or stationary) may experience long partitioning periods before contacting each other or some info-stations. Within the same context of underwater sensing, there is the example of SeaWeb, a project conducted by the U.S. Navy. SeaWeb has developed its own MAC layer protocol, especially optimized for the acoustic networking case. The nodes in the SeaWeb have been mainly disposable in that they run on batteries with no possibility for recharging.

3. **Village network**
   Rural areas have limitations of lacking of infrastructure. Village networks represent a very promising public application for DTNs, especially in secluded areas lacking communication infrastructure. Rural buses may be also used to provide Internet connectivity to isolated and remote villages. Busses act here as relays or couriers, transmitting and exchanging data via simple wireless transmission across the cities bus network. Like in the SeaWeb example, several other connectivity options may be integrated here (e.g. satellites, LEO, GEO, telephones) to aid the delivery process.

4. **Interplanetary network**
   The massive distances separating terrestrial artificial objects and the need for these objects to exchange data among each other or with base-stations on earth –or perhaps other planets–represent an extreme case of DTN communication. NASA’s vision of an Inter-Planetary Network (IPN) that initiated the search for a heterogeneous architecture that overcomes the traditional limitations of TCP, which eventually evolved into the DTN field of research. The combination of long signal propagation times and intermittent connectivity caused by the interposition of a planetary body between the sender and the receiver can result in round-trip communication delays measured not in milliseconds or even minutes but in hours or days.
5. Military applications

There is a need to monitor extended geographical planes, their objects and inhabitants-i.e. soldiers-who would be equipped with wireless sensors in order to indicate their locations. Battlefields are dangerous. While it would be acceptable to assume human interference in collecting data from the nodes (e.g. an info-station is driven close enough to zebra herds to allow for wireless interaction), it is expected that a higher level of automation is presented in military application. Tactical military networks are established in a very Ad Hoc manner. The nodes are in continuous and rapid motion. And there is most likely no stable infrastructure due since such infrastructure would just provide a target for the enemy.

III. STORE-CARRY-FORWARD MECHANISM

DTN works on the principle of store-carry and forward mechanism. Delay Tolerant Networks have overcome the problems associated with the conventional protocols using the concept of store-carry and forward method.

![Store-carry-forward mechanism](image1)

**Figure 3.1 : Store-carry-forward mechanism**

Under this paradigm, each node in the network stores a packet that has been forwarded to it by another node, carries the packet while moves around, and forward it to other relay nodes or to the destination node when they come within transmission range. DTN nodes utilize store-carry messages can be sent over an existing link and buffered at the next hop until the next link in path appears. It is similar to postal service, every letter has to pass through a set of post offices, here it is processed and forwarded, before reach destination. Here complete message of it is transferred and stored in nodes successively until it reaches the destination.

**Blackhole attacks**

DTN is vulnerable to blackhole and greyhole attacks, due to the limited connectivity. Blackhole attackers drop all the received messages even if they have enough buffer storage. Attacker can drop received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. Blackhole Attack is a “passive” and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a packet every \( n \) packets, a packet every \( t \) seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

![Blackhole attacks](image2)

**Figure 3.2 : Blackhole attacks**
Greyhole attacks

Greyhole attackers drop a fraction of received messages to avoid arousing suspicion and detection from other nodes. In greyhole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. The dropping misbehaviour will decrease the overall message delivery and waste the resources of intermediate nodes that have carried and forwarded the dropped messages. DTN makes use of hop-by-hop routing and the store-and-forward paradigm to overcome the lack of end-to-end paths.

![Diagram of Greyhole attacks](image)

**Figure 3.3**: Greyhole attacks

**Individual attacks**

An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of a useful data.

**Collusion attacks**

Malicious nodes are cooperate with each other to cheat the defense system called as colluding attackers, who misbehaving with the normal nodes by creating fake records for each other called as collusion attacks.

**IV. LITERATURE SURVEY**

In 2001, Dan Boneh and Matt Franklin focuses on the ciphertext security in random oracle model as an elliptic curve. This security model is based on a natural analogue of the computational Diffie-Hellman assumption and also uses standard techniques from threshold cryptography, PKG (Private Key Generator) can be distributed so that master key is not available in a single location.

In 2005, Fani Tsapeli and Vassilis Tsaoussidis focused on redundancy scheme which is used to enhance reliability and reduces delivery delay which spread multiple copies of message in network. Transmission of multiple copies results in wastage of network resources, which increases traffic overhead. To overcome this, Erasure coding has been developed, to generate redundancy instead of replication. In this technique, each message is encoded into number of code blocks, this reconstruction of the original message requires only a specific amount of the generated code blocks.

In the same year, Yong Wang, Sushant Jain, Margaret Martonosi, Kevin Fall proposed a scheme that improves delay performance. Conceptually it erasure code a message and distributes that code-blocks over a large number of relays. Sending a full copy of the message over a relay if compared, only a fraction of code-blocks are sent over each relay. The routing overhead is controlled by allowing this fraction of code-blocks in terms of transmitted bytes.

In 2006, Shuchita Upadhyaya and Karishma proposed a Cooperative mechanism that detects blackhole attack in which each node maintains the history that includes message delivery rate of that node and this rate will determine a CFV i.e. Combined Faith Value separately. When a sending node wants to send packet, all its neighbour nodes give their opinion whether the node was chosen to send the packet. Faith value is obtained by this opinion and this value compared with a predefined value.
If the faith value is below than minimum value then that node is considered as a blackhole otherwise it is a normal node.

In 2007, Simbet DTN routing algorithm is a social based routing protocol which is proposed by Elizabeth Daly and Mads Haahr. It determines some bridge nodes in the network using betweeness centrality and similarity metrics. The algorithm in Simbet routing represents the communication between the two nodes.

In the same year, M. Chuah, P. Yang, J. Han was introduced FBIDM which is used with custody transfer feature when a multihop routing scheme used. This scheme doesn’t perform well when history based routing schemes are used. So FBIDM can run history based routing schemes e.g. Prophet, Maxprop. The geographical area is divided into multiple cells and has ferries visit the center of each cell using some fixed routes, for the single ferry and two ferries. Each ferry stops at a few locations within its route. At each location, the ferry will broadcast a secret service message that each legitimate node knows deciphering.

In 2008, Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin–Han Ho, Xuemin (Sherman) Shen was introduced SLAB scheme for addressing ensure of security and system performance. Also this scheme takes the merits of the PKI architecture for constructing the trust mechanism between various Internet Service Providers and wireless service providers and mobile user using roaming brokers.

In 2009, Haojin Zhu, Xiaodong Lin, Rongxing Lu, Yanfei Fan, and Xuemin (Sherman) Shen focuses on A SMART uses credits for providing incentives to selfish nodes in the network. It stimulates bundle forwarding cooperation among DTN nodes and can be implemented in a distributed manner for thwart different attacks without relying on tamperproof hardware. This scheme is based on the notion of layered coin which provides the virtual electronic credits, composed of various multiple attacks. Each layer is produced by the source or intermediate or destination node.

In the same year, Feng Li, Jie Wu, Avinash Srinivasan defines Encounter tickets that are introduced for routing and packet forwarding, when two nodes meet, they generate an encounter ticket that carries a timestamp. Based on trusted PKI, two nodes sign the ticket with their private keys. When a node history reveals with another node, it submits the encounter tickets instead of a compressed list containing only node ID’s and the number of contacts previously employed. This is the ticket based history interpretation scheme.

In 2010, Rongxin Lu, Xiaodong Lin, Haojin Zhu, Xuemin (Sherman) Shen developed an Practical incentive protocol called Pi. This protocol is used for addressing the selfishness problem in DTN. Pi can be used to improve the performance of DTN in the terms of low average delay and high delivery ratio. The Pi attaches some incentive on the bundle when source node sends a bundle message which is fair to all participating DTN nodes. It provides various security issues such as fair incentive, layer adding attack and layer removing attack.

In the same year, Theus Hossmann, Thrasyvoulos Spyropoulos, and Franck Legendre introduced an online algorithm that uses concepts from unsupervised learning and spectral graph theory to infer “correct” graph structure. This algorithm allows each node to identify and adjust to the optimal operating point. Complex Network Analysis (CNA) has been proposed as more genetic and powerful tool to formulate and solve the problem of future contact prediction in DTN. CNA metrics are used by two routing protocols, Simbet and BubbleRap, which highlights a node’s position in the aggregated destined to other nodes in the graph.

In the same year, Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen was developed Mutual correlation detection scheme (MUTON) to address insider attacks. The transitive property of MUTON considers when calculating the packet delivery probability of each node and correlates the information collected from other nodes. Each node collects the packet delivery probabilities of any node that it encounters with and past encounter history of that node. The collected information is used for estimating the changes in the delivery probabilities to other nodes. During detection, when the ferry encounters a node, it uses a self-examination approach.
Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen introduced the detection scheme that only utilizes the network topology information for detecting a wormhole attack. Nodes in the network will reduce their transmission range for a minimum period of time. The detection of the presence of a forbidden structure is caused by a wormhole attack that cannot be present under normal situations without attacks.

In the same year, Erman Ayday, Hanseung Lee, Faramarz Fekri introduced a security mechanism for DTN enables to detect misbehavior due to Byzantine adversaries. So that a reputation based trust management system and an iterative malicious node detection mechanism for DTN has been developed. The work on global reputation system implements in the use of iterative algorithm such as message passing techniques in the decoding of Low-Density Parity Check(LDPC) codes in Erasure channels. A distributed malicious node detection mechanism was proposed using ITRM (Iterative Trust and Reputation Mechanism) which enables every node to evaluate other nodes based on their past behavior.

In 2011, Wei Gao and Guohong Cao introduced the concept of user-centric data dissemination in DTN considers satisfying user interests and forwards data only to the nodes that are interested in data. The node centrality in DTN is consider as social contact patterns and interests of mobile nodes for effective relay selection. While centrality in Social Network Analysis (SNA), generally represents the capability of a node facilitating the social communication among other nodes.

In the same year, Lifei Wei, Haojin Zhu, Zhenfu Cao, and Xuemin (Sherman) Shen developed MobiID to solve incentive issue in DTN which is challenging due to the unique network characteristics. MobiID allows a node to manage its reputation evidence. To speed up reputation establishment, the self-check and community-check was defined. MobiID stimulate cooperation among selfish nodes in DTN. MobiID is a dynamic reputation system where reputation can be maintained, updated and shown for verification by each node whenever needed.

In 2012, Qinghua Li and Guohong Cao proposed scheme that detects packet dropping in a distributed manner. A node is required to keep previous signed contact records i.e. the buffered packets that are sent or received and report them to the next contact node. This node can detect whether the node has dropped packets based on the reported records. To detect consistency, a small part of each contact record is disseminated to selected nodes, collect appropriate contact records and detect misbehaving nodes with certain probability.

In 2016, Mythili M., Renuka K. Developed a scheme that detects different types of attack on DTN such as blackhole and greyhole attacks using fuzzy rule. This detection system is based on Fuzzy Logic. An IDS system is improved by making use of two factors i.e. packet loss rate, data rate. They use both factors with fuzzy logic to solve problem using problem solving control system. In this, a fuzzy algorithm is used to detect attack.

Table 1: Various Attack Detection Techniques

<table>
<thead>
<tr>
<th>YEAR</th>
<th>AUTHOR</th>
<th>PARAMETER</th>
<th>CONTRIBUTION</th>
<th>ATTACKS DETECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007 [20]</td>
<td>M. Chuah, P. Yang, and J. Han</td>
<td>Ferry node, delivery probability, insider attacks</td>
<td>The scheme (FBIDM) is used to detect blackhole attacks in DTN using trusted examiner, ferry node. Trusted ferries collect the history of latest delivery predictability values of different nodes and cross-check the consistency of claims from different nodes.</td>
<td>blackhole attack, individual attack</td>
</tr>
<tr>
<td>Year</td>
<td>Authors</td>
<td>Metrics</td>
<td>Description</td>
<td>Attack Type</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2009</td>
<td>F. Li, J. Wu, and A. Srinivasan</td>
<td>Encounter records, routing metrics</td>
<td>In this scheme, authenticated encounter records make it impossible for the adversary to claim non-existent encounters and abuse them to forge routing metrics to attract data.</td>
<td>Individual attack</td>
</tr>
<tr>
<td>2010</td>
<td>Y. Ren, M. Chuah, J. Yang, and Y. Chen</td>
<td>Detection time, number of malicious nodes, self-examination approach</td>
<td>A mutual correlation detection scheme (MUTON) is used for addressing insider attacks.</td>
<td>Blackhole attack, insider attack</td>
</tr>
<tr>
<td>2012</td>
<td>Q. Li and G. Cao</td>
<td>Detection, mitigation, routing misbehavior</td>
<td>In this scheme, each contact record records the initial message buffer, sent and received messages during an encounter. A misbehaving node dropping packets received from the previous contacted node, will be detected by the next contacted node.</td>
<td>Individual attack</td>
</tr>
<tr>
<td>2013</td>
<td>Y. Guo, S. Schildt, and L. Wolf</td>
<td>Delivery rate, detection rate, encounter records</td>
<td>This scheme is based on encounter records to estimate the forwarding ratios. It detects both blackhole and greyhole behaviors with high detection rate.</td>
<td>Individual attack, blackhole and greyhole attack</td>
</tr>
<tr>
<td>2013</td>
<td>N. Li and S. K. Das</td>
<td>Opportunistic network, routing protocol</td>
<td>This scheme uses a distributed trust-based framework in which the forwarding behavior of a node is acknowledged by its next hop and a forwarding receipt is sent out to other nodes to update its reputation.</td>
<td>Individual attack, blackhole and greyhole attack</td>
</tr>
<tr>
<td>2014</td>
<td>Z. Gao, H. Zhu, S. Du, C. Xiao and R. Lu</td>
<td>Detection cost, detection performance, inspection probability, punishment and compensation</td>
<td>A probabilistic misbehavior detection scheme (PMDS) is used to detect misbehaviour in DTN, and collects relevant secured evidences like contact over network.</td>
<td>Individual attack, blackhole and greyhole attack</td>
</tr>
</tbody>
</table>
V. ANALYSIS OF ATTACK DETECTION TECHNIQUES

I have studied and analyze these attack detection techniques for DTN such as FBIDM, Encounter ticket based scheme, MUTON, Distributed scheme, Trust based framework, PMDS and so on. It is clear that there is a need to develop a scheme which can defend against collusion attacks. Table 2 shows the work which requires further attention as well as the work which has already been attempted by different researchers in the area of blackhole and greyhole attack detection with collusion attack detection.

✓: Tick sign show that work has already been done in that area
?
: Question mark means that there need to develop a scheme which can defend against collusion attacks.

Table 2: Analysis of different attack detection techniques

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Individual attack</th>
<th>Blackhole attack</th>
<th>Greyhole attack</th>
<th>Collusion attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>FBIDM</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Encounter ticket based scheme</td>
<td>✓</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>MUTON</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Distributed scheme</td>
<td>✓</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Trust based framework</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>PMDS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
</tr>
</tbody>
</table>

VI. CONCLUSION

In this paper, I have surveyed various attack detection techniques in Delay Tolerant Network and compared them. From the literature reviewed, it is clear that a lot of work has been done in this area but there is a need to develop a scheme to detect collusion attacks.

REFERENCES


